

USER MANUAL

COMPREHENSIVE IT MONITORING TO SIMPLIFY THE ADMIN'S DAILY WORK

PRTG Network Monitor User Manual

© 2018 Paessler AG

All rights reserved. No parts of this work may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: August 2018 in Nuremberg

Table of Contents

Part 1	Welcome to PRTG Network Monitor	14
1	About this Document	16
2	Key Features	17
3	New in This Version	20
4	Available Licenses	21
5	System Requirements	23
	Detailed System Requirements	26
6	Introduction: Monitoring with PRTG	34
Part 2	Quick Start Guide	46
1	ONE—Download, Installation, and First Login	48
2	TWO—Smart Setup	52
Part 3	Using PRTG Hosted by Paessler	62
1	Create a PRTG Hosted by Paessler Instance	63
2	Manage a PRTG Hosted by Paessler Subscription	71
Part 4	Installing the Software	80
1	Download PRTG	81
2	Update From Previous Versions	83
3	Install a PRTG Core Server	89
4	Install a PRTG Cluster	95
5	Enter a License Key	96
6	Activate the Product	99
7	Install a PRTG Remote Probe	101
8	Install the Enterprise Console	113
9	Uninstall PRTG Products	119
Part 5	Understanding Basic Concepts	124
1	Architecture and User Interfaces	125
2	Clustering	130
3	Object Hierarchy	133
4	Inheritance of Settings	137
5	Tags	139
6	Dependencies	141
7	Scheduling	142
8	Notifying	143
	Alerts	144
9	User Access Rights	158
10	Data Reporting	162
11	IPv6	163

Part 6 Ajax Web Interface—Basic Procedures 166

1	Login	168
2	SSL Certificate Warning	172
3	Welcome Page	175
	Customer Service	178
4	General Layout	181
5	Sensor States	195
6	Review Monitoring Data	198
7	Historic Data Reports	204
8	Similar Sensors	209
9	Recommended Sensors	213
10	Object Settings	217
11	Alarms	219
12	System Information	222
13	Logs	228
14	Tickets	230
15	Working with Table Lists	237
16	Object Selector	240
17	Priority and Favorites	242
18	Pause	245
19	Context Menus	247
20	Hover Popup	262
21	Main Menu Structure	263

Part 7 Ajax Web Interface—Device and Sensor Setup 280

1	Auto-Discovery	282
2	Create Objects Manually	301
	Add a Group	302
	Add a Device	311
	Add a Sensor	325
3	Manage Device Tree	329
4	Root Group Settings	331
5	Probe Settings	351
6	Group Settings	375
7	Device Settings	402
8	Sensor Settings	428
	List of Available Sensor Types	429
	Active Directory Replication Errors Sensor	453
	ADO SQL v2 Sensor	463
	Amazon CloudWatch Alarm Sensor	479
	Amazon CloudWatch EBS Sensor	489
	Amazon CloudWatch EC2 Sensor	501
	Amazon CloudWatch ElastiCache Sensor	514
	Amazon CloudWatch ELB Sensor	527
	Amazon CloudWatch RDS Sensor	539
	Amazon CloudWatch SNS Sensor	552

Contents

Amazon CloudWatch SQS Sensor	564
Business Process Sensor	576
Cisco IP SLA Sensor	589
Citrix XenServer Host Sensor	599
Citrix XenServer Virtual Machine Sensor	609
Cloud HTTP Sensor	619
Cloud Ping Sensor	629
Cluster Health Sensor	638
Common SaaS Sensor	644
Core Health Sensor	652
Dell PowerVault MDi Logical Disk Sensor	659
Dell PowerVault MDi Physical Disk Sensor	669
DHCP Sensor	680
DICOM Bandwidth Sensor	691
DICOM C-ECHO Sensor	701
DICOM Query/Retrieve Sensor	710
DNS Sensor	721
Docker Container Status Sensor	730
Dropbox Sensor	741
Enterprise Virtual Array Sensor	751
Event Log (Windows API) Sensor	761
Exchange Backup (Powershell) Sensor	773
Exchange Database (Powershell) Sensor	783
Exchange Database DAG (Powershell) Sensor	794
Exchange Mail Queue (Powershell) Sensor	804
Exchange Mailbox (Powershell) Sensor	814
Exchange Public Folder (Powershell) Sensor	824
EXE/Script Sensor	834
EXE/Script Advanced Sensor	847
File Sensor	860
File Content Sensor	870
Folder Sensor	880
FTP Sensor	891
FTP Server File Count Sensor	900
GitLab Build Status Sensor	911
Google Analytics Sensor	921
Google Drive Sensor	934
HL7 Sensor	944
HTTP Sensor	955
HTTP Advanced Sensor	965
HTTP Apache ModStatus PerfStats Sensor	982
HTTP Apache ModStatus Totals Sensor	992
HTTP Content Sensor	1002
HTTP Data Advanced Sensor	1014
HTTP Full Web Page Sensor	1027
HTTP IoT Push Data Advanced	1038
HTTP Push Count Sensor	1049
HTTP Push Data Sensor	1059
HTTP Push Data Advanced Sensor	1070
HTTP Transaction Sensor	1081
HTTP XML/REST Value Sensor	1095

Hyper-V Cluster Shared Volume Disk Free Sensor	1110
Hyper-V Host Server Sensor	1121
Hyper-V Virtual Machine Sensor	1130
Hyper-V Virtual Network Adapter Sensor	1141
Hyper-V Virtual Storage Device Sensor	1152
IMAP Sensor	1162
IP on DNS Blacklist Sensor	1177
IPFIX Sensor	1186
IPFIX (Custom) Sensor	1200
IPMI System Health Sensor	1213
jFlow V5 Sensor	1223
jFlow V5 (Custom) Sensor	1237
LDAP Sensor	1250
Microsoft OneDrive Sensor	1257
Microsoft SQL v2 Sensor	1267
MySQL v2 Sensor	1284
NetApp Aggregate Sensor	1300
NetApp I/O Sensor	1311
NetApp LIF Sensor	1323
NetApp LUN Sensor	1334
NetApp NIC Sensor	1345
NetApp Physical Disk Sensor	1356
NetApp SnapMirror Sensor	1367
NetApp System Health Sensor	1379
NetApp Volume Sensor	1391
NetFlow V5 Sensor	1403
NetFlow V5 (Custom) Sensor	1417
NetFlow V9 Sensor	1430
NetFlow V9 (Custom) Sensor	1444
Oracle SQL v2 Sensor	1457
Oracle Tablespace Sensor	1474
Packet Sniffer Sensor	1484
Packet Sniffer (Custom) Sensor	1497
PerfCounter Custom Sensor	1509
PerfCounter IIS Application Pool Sensor	1519
Ping Sensor	1529
Ping Jitter Sensor	1538
POP3 Sensor	1547
Port Sensor	1556
Port Range Sensor	1566
PostgreSQL Sensor	1574
Probe Health Sensor	1590
Python Script Advanced Sensor	1597
QoS (Quality of Service) One Way Sensor	1608
QoS (Quality of Service) Round Trip Sensor	1617
RADIUS v2 Sensor	1628
RDP (Remote Desktop) Sensor	1638
REST Custom Sensor	1646
REST Dell EMC Capacity Sensor	1671
REST Dell EMC File System Sensor	1680
REST Dell EMC LUN Sensor	1690

Contents

REST Dell EMC Pool Sensor	1700
REST Dell EMC System Health Sensor	1711
Sensor Factory Sensor	1720
sFlow Sensor	1740
sFlow (Custom) Sensor	1754
SFTP Secure File Transfer Protocol Sensor	1767
Share Disk Free Sensor	1777
SIP Options Ping Sensor	1786
SMTP Sensor	1795
SMTP&IMAP Round Trip Sensor	1805
SMTP&POP3 Round Trip Sensor	1817
SNMP APC Hardware Sensor	1829
SNMP Buffalo TS System Health Sensor	1838
SNMP Cisco ADSL Sensor	1847
SNMP Cisco ASA VPN Connections Sensor	1856
SNMP Cisco ASA VPN Traffic Sensor	1866
SNMP Cisco ASA VPN Users Sensor	1877
SNMP Cisco CBQoS Sensor	1887
SNMP Cisco System Health Sensor	1896
SNMP Cisco UCS Blade Sensor	1905
SNMP Cisco UCS Chassis Sensor	1914
SNMP Cisco UCS Physical Disk Sensor	1923
SNMP Cisco UCS System Health Sensor	1932
SNMP CPU Load Sensor	1941
SNMP Custom Sensor	1949
SNMP Custom Advanced Sensor	1959
SNMP Custom String Sensor	1970
SNMP Custom String Lookup Sensor	1982
SNMP Custom Table Sensor	1992
SNMP Dell EqualLogic Logical Disk Sensor	2004
SNMP Dell EqualLogic Member Health Sensor	2013
SNMP Dell EqualLogic Physical Disk Sensor	2023
SNMP Dell Hardware Sensor	2032
SNMP Dell PowerEdge Physical Disk Sensor	2042
SNMP Dell PowerEdge System Health Sensor	2052
SNMP Disk Free Sensor	2063
SNMP Fujitsu System Health Sensor	2072
SNMP Hardware Status Sensor	2082
SNMP HP BladeSystem Blade Sensor	2091
SNMP HP BladeSystem Enclosure System Health Sensor	2100
SNMP HP LaserJet Hardware Sensor	2108
SNMP HP ProLiant Logical Disk Sensor	2117
SNMP HP ProLiant Memory Controller Sensor	2126
SNMP HP ProLiant Network Interface Sensor	2136
SNMP HP ProLiant Physical Disk Sensor	2146
SNMP HP ProLiant System Health Sensor	2156
SNMP IBM System X Logical Disk Sensor	2166
SNMP IBM System X Physical Disk Sensor	2175
SNMP IBM System X Physical Memory Sensor	2184
SNMP IBM System X System Health Sensor	2193
SNMP interSeptor Pro Environment Sensor	2203

SNMP Juniper NS System Health Sensor	2212
SNMP LenovoEMC Physical Disk Sensor	2220
SNMP LenovoEMC System Health Sensor	2229
SNMP Library Sensor	2237
SNMP Linux Disk Free Sensor	2251
SNMP Linux Load Average Sensor	2263
SNMP Linux Meminfo Sensor	2271
SNMP Linux Physical Disk Sensor	2279
SNMP Memory Sensor	2288
SNMP NetApp Disk Free Sensor	2297
SNMP NetApp Enclosure Sensor	2306
SNMP NetApp I/O Sensor	2316
SNMP NetApp License Sensor	2325
SNMP NetApp Logical Unit Sensor	2334
SNMP NetApp Network Interface Sensor	2343
SNMP NetApp System Health Sensor	2352
SNMP Poseidon Environment Sensor	2361
SNMP Printer Sensor	2370
SNMP QNAP Logical Disk Sensor	2378
SNMP QNAP Physical Disk Sensor	2387
SNMP QNAP System Health Sensor	2396
SNMP RMON Sensor	2405
SNMP SonicWall System Health Sensor	2416
SNMP SonicWall VPN Traffic Sensor	2424
SNMP Synology Logical Disk Sensor	2433
SNMP Synology Physical Disk Sensor	2442
SNMP Synology System Health Sensor	2451
SNMP System Uptime Sensor	2459
SNMP Traffic Sensor	2467
SNMP Trap Receiver Sensor	2479
SNMP Windows Service Sensor	2492
SNTTP Sensor	2500
SSH Disk Free Sensor	2507
SSH INodes Free Sensor	2522
SSH Load Average Sensor	2532
SSH Meminfo Sensor	2542
SSH Remote Ping Sensor	2552
SSH SAN Enclosure Sensor	2562
SSH SAN Logical Disk Sensor	2573
SSH SAN Physical Disk Sensor	2584
SSH SAN System Health Sensor	2596
SSH Script Sensor	2607
SSH Script Advanced Sensor	2622
SSL Certificate Sensor	2635
SSL Security Check Sensor	2646
Syslog Receiver Sensor	2656
System Health Sensor	2669
TFTP Sensor	2675
Traceroute Hop Count Sensor	2683
VMware Datastore (SOAP) Sensor	2692
VMware Host Hardware (WBEM) Sensor	2703

Contents

VMware Host Hardware Status (SOAP) Sensor	2713
VMware Host Performance (SOAP) Sensor	2723
VMware Virtual Machine (SOAP) Sensor	2733
Windows CPU Load Sensor	2744
Windows IIS 6.0 SMTP Received Sensor	2754
Windows IIS 6.0 SMTP Sent Sensor	2763
Windows IIS Application Sensor	2772
Windows MSMQ Queue Length Sensor	2782
Windows Network Card Sensor	2793
Windows Pagefile Sensor	2805
Windows Physical Disk I/O Sensor	2815
Windows Print Queue Sensor	2826
Windows Process Sensor	2837
Windows System Uptime Sensor	2848
Windows Updates Status (Powershell) Sensor	2857
WMI Custom Sensor	2867
WMI Custom String Sensor	2877
WMI Event Log Sensor	2889
WMI Exchange Server Sensor	2902
WMI Exchange Transport Queue Sensor	2913
WMI File Sensor	2924
WMI Free Disk Space (Multi Disk) Sensor	2933
WMI HDD Health Sensor	2945
WMI Logical Disk I/O Sensor	2956
WMI Memory Sensor	2966
WMI Microsoft SQL Server 2005 Sensor (Deprecated)	2975
WMI Microsoft SQL Server 2008 Sensor	2988
WMI Microsoft SQL Server 2012 Sensor	3000
WMI Microsoft SQL Server 2014 Sensor	3012
WMI Microsoft SQL Server 2016 Sensor	3024
WMI Microsoft SQL Server 2017 Sensor	3036
WMI Remote Ping Sensor	3048
WMI Security Center Sensor	3057
WMI Service Sensor	3067
WMI Share Sensor	3077
WMI SharePoint Process Sensor	3088
WMI Terminal Services (Windows 2008+) Sensor	3097
WMI Terminal Services (Windows XP/Vista/2003) Sensor	3106
WMI UTC Time Sensor	3115
WMI Vital System Data (V2) Sensor	3124
WMI Volume Sensor	3134
WSUS Statistics Sensor	3144
9 Additional Sensor Types (Custom Sensors)	3155
10 Sensor Channels Settings	3160
11 Sensor Notification Triggers Settings	3170
Part 8 Ajax Web Interface—Advanced Procedures	3184
1 Toplists	3186
2 Arrange Objects	3191
3 Clone Object	3193

4	Multi-Edit	3197
5	Create Device Template	3203
6	Show Dependencies	3209
7	Geo Maps	3211
8	Notifications	3216
	Setting up Notifications Based on Sensor Limits: Example	3219
	Setting up Notifications Based on Libraries: Example	3229
9	Libraries	3235
	Libraries Step By Step	3238
	Management	3242
	Libraries and Node Settings	3245
	Context Menus	3251
10	Reports	3252
	Reports Step By Step	3257
	View and Run Reports	3261
	Report Settings	3265
11	Maps	3278
	Maps Step By Step	3283
	Map Designer	3287
	Maps Settings	3297
12	Setup	3302
	Account Settings—My Account	3304
	Account Settings—Notification Templates	3311
	Account Settings—Notification Contacts	3334
	Account Settings—Schedules	3338
	System Administration—User Interface	3343
	System Administration—Monitoring	3355
	System Administration—Notification Delivery	3361
	System Administration—Core & Probes	3368
	System Administration—User Accounts	3376
	System Administration—User Groups	3383
	System Administration—Administrative Tools	3388
	System Administration—Cluster	3394
	PRTG Status—System Status	3396
	PRTG Status—Auto-Update	3407
	PRTG Status—Cluster Status	3412
	PRTG Status—Licensing Status and Settings	3414
	Optional Downloads and Tools	3420
	Desktop Notifications	3422
	Support—Contact Support	3424

Part 9 Enterprise Console **3430**

1	First Start	3433
2	General Layout	3434
3	Menu Tabs and Page Content	3438
	Devices	3439
	Libraries	3446
	Sensors	3448
	Alarms	3450

Maps	3452
Reports	3454
Logs	3456
Tickets	3458
Setup	3460
Search Results	3462
4 PRTG Servers	3463
5 Options	3466
6 Windows Menu Structure	3472
7 Context Menus	3480
8 Shortcuts Overview	3481
Part 10 PRTG Apps for Mobile Network Monitoring	3484
Part 11 Sensor Technologies	3488
1 Monitoring via SNMP	3489
Choosing the Right SNMP Sensor	3494
2 Monitoring via WMI	3507
3 Monitoring via SSH	3510
4 Monitoring Bandwidth via Packet Sniffing	3512
5 Monitoring Bandwidth via Flows	3514
6 Bandwidth Monitoring Comparison	3517
7 Monitoring Quality of Service and VoIP	3519
8 Monitoring Email Round Trip	3524
9 Monitoring Backups	3526
10 Monitoring Virtual Environments	3527
11 Monitoring Databases	3534
12 Monitoring Syslogs and SNMP Traps	3539
13 Monitoring via Push	3548
14 Monitoring via HTTP	3552
Part 12 PRTG Administration Tool	3560
1 PRTG Administration Tool on Core Server System	3561
2 PRTG Administration Tool on Remote Probe Systems	3587
Part 13 Advanced Topics	3602
1 Active Directory Integration	3603
2 Application Programming Interface (API) Definition	3606
HTTP API	3607
Live Data	3610
Live Graphs	3625
Historic Data	3628
Object Manipulation	3631
Custom Sensors	3637
Custom Notifications	3658
Mini Probe API	3660
3 Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors	3685

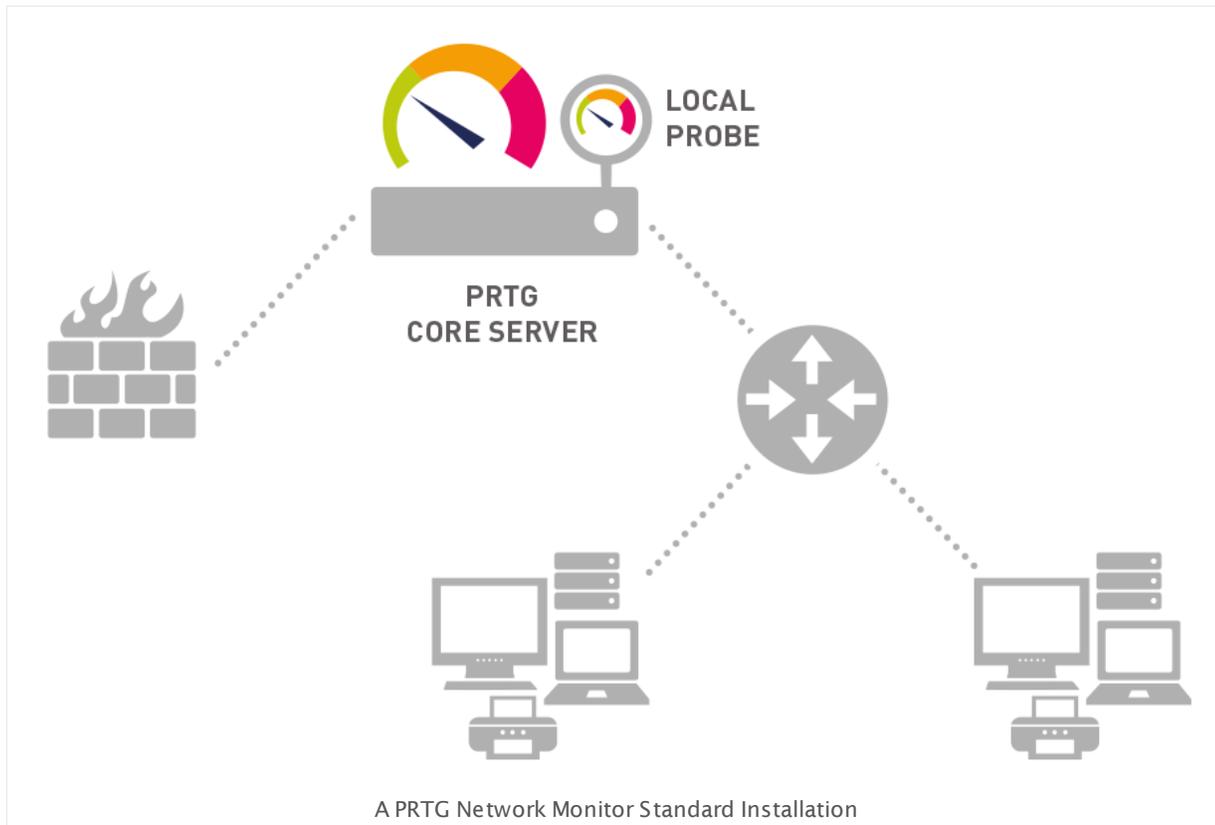
4	Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors	3690
5	Define IP Ranges	3692
6	Define Lookups	3693
7	Regular Expressions	3704
8	Calculating Percentiles	3706
9	Add Remote Probe	3707
	Remote Probes and Multiple Probes	3709
	Remote Probe Quick Setup	3713
	Remote Probe Setup Using Installer	3719
10	Failover Cluster Configuration	3720
	Failover Cluster Step by Step	3727
11	Data Storage	3734
12	Using Your Own SSL Certificate with PRTG's Web Server	3736
Part 14	Appendix	3740
1	Glossary	3741
2	List of Abbreviations	3749
3	List of Icons	3754
4	Support and Troubleshooting	3755
5	Differences between PRTG on Premises and PRTG Hosted by Paessler	3756
6	Legal Notices	3766

Part 1

Welcome to PRTG Network Monitor

1 Welcome to PRTG Network Monitor

Welcome to PRTG Network Monitor! You have chosen an easy-to-use software product that comes with a powerful set of features to monitor your entire network.



Why Network Monitoring is Important

Today, nearly every business relies on a computer and network infrastructure for internet, internal management, telephone, and email. A complex set of servers and network equipment is required to ensure that business data flows seamlessly between employees, offices, and customers. The economic success of an organization is tightly connected to a hitch-free flow of data.

That's why your computer network has to work successfully: reliability, speed, and efficiency are crucial. But, like all other technical objects, network devices may fail from time to time—potentially causing trouble and loss of sales, no matter what migration efforts have been made up-front.

So network administrators need to take three key steps to maintain network uptime, reliability, and speed:

1. Set up a well-planned network with reliable components.
2. Create recovery plans for the event of device failure.

3. Monitor the network to get informed about failures when they build up or actually happen.

PRTG Network Monitor, the software described in this document, is a **complete solution** for monitoring **small, medium, and large networks**.

Monitoring Networks with PRTG Network Monitor

PRTG Network Monitor is a powerful network monitoring application for Windows-based systems. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN, and VPN monitoring. You can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more.

PRTG monitors network availability and bandwidth usage, as well as various other network parameters such as quality of service, memory load, and CPU usages, even on remote machines. PRTG provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

The software is easy to set up and use and monitors a network using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffer, Cisco NetFlow (as well as IPFIX, sFlow, and jFlow), and many other industry standard protocols. It runs on a Windows-based machine in your network for 24 hours every day. PRTG Network Monitor constantly records the network usage parameters and the availability of network systems. The recorded data is stored in an internal database for later analysis.

PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG hosted by Paessler. With PRTG on premises, the core server and local probe run within your network. PRTG hosted by Paessler is the PRTG cloud solution, where we at Paessler run the core server and hosted probe for you. The [PRTG web interface](#) for monitoring configuration and reviewing monitoring data is the same for both, PRTG hosted by Paessler and PRTG on premises.

 Do you want to get an overview of PRTG in 90 seconds? See this video on our website: [PRTG Network Monitor in 90 Seconds](#)

More

Video Demo: PRTG Network Monitor in 90 Seconds

- <https://www.paessler.com/support/videos/about-paessler/prtg-90-sec>

Video Demo: What is Unified Monitoring?

- <https://www.paessler.com/support/videos/all-about-monitoring>

1.1 About this Document

This document introduces you to the system concepts of **PRTG Network Monitor** and explains how to set up the software to achieve the best monitoring results. You will learn how to plan your monitoring setup, how to set up your devices and sensors, dependencies, reports, notifications, maps, user accounts, and clustering for fail-safe monitoring.

This document is also meant to be a reference for all available settings in PRTG. Short contextual help is already provided within the Ajax web interface of PRTG. In this manual you often get some more help regarding the different options that are available. No matter whether you use PRTG hosted by Paessler or PRTG on premises, you will find all of the information that you need in this document.

This document does **not** explain monitoring protocols and file formats in-depth. Also, the use of the Application Programming Interface (API) built into PRTG is only briefly addressed. Whenever possible, hyperlinks to more detailed resources are provided, such as articles in the [Paessler Knowledge Base](#).

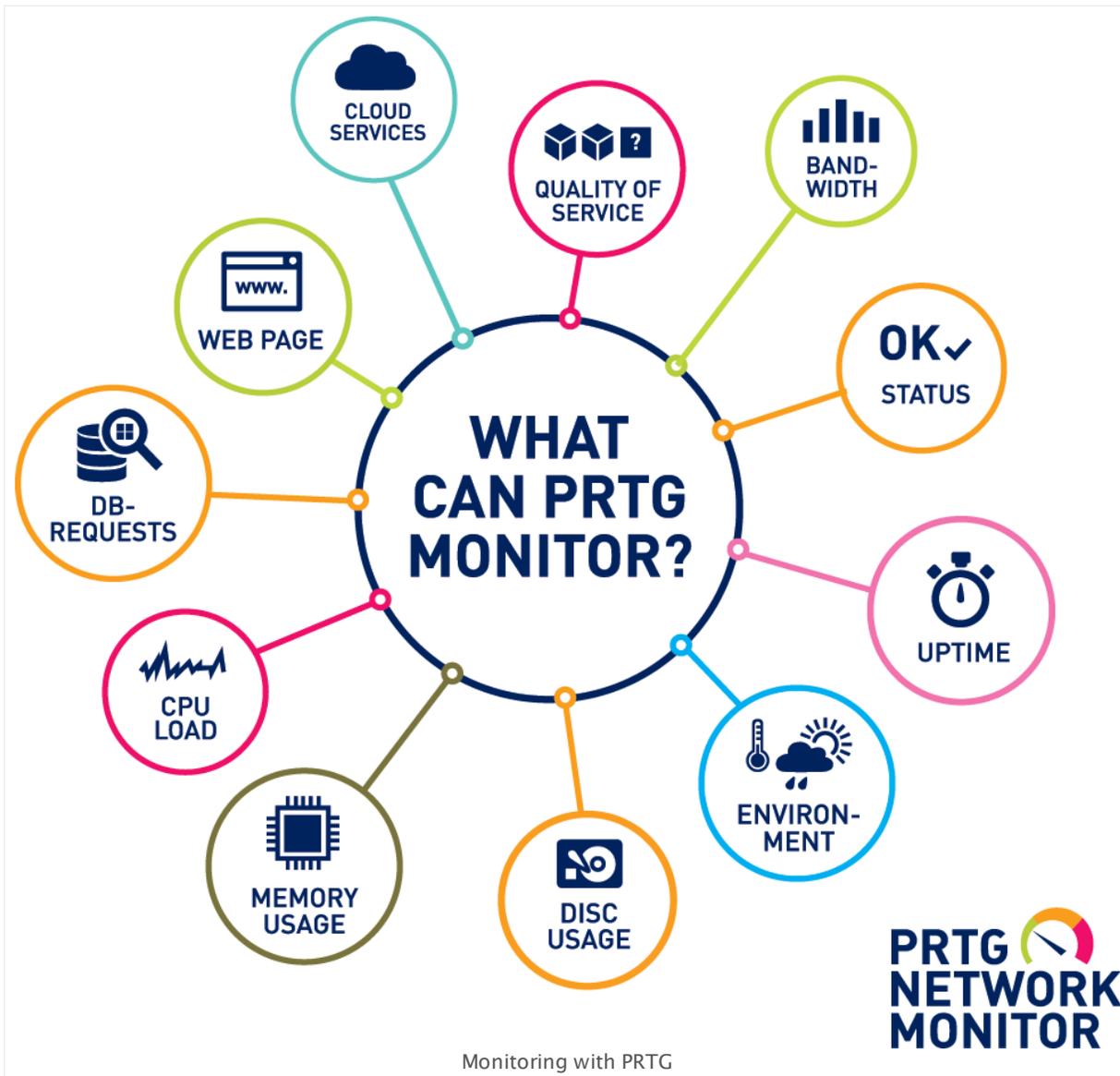
 To start using PRTG right away, see the [Quick Start Guide](#)^[46] section. To learn more about monitoring with PRTG, see section [Introduction: Monitoring with PRTG](#)^[34]. For more detailed instructions, browse the manual content or use the manual search with keywords and choose the section you want to read.

 For an overview of the icons and abbreviations that are used in this document, see the [Appendix](#)^[3740] section.

1.2 Key Features

PRTG Network Monitor follows and analyzes your network and requires no third-party software. It's quick to download and install, or you create a PRTG instance in the cloud, hosted by Paessler, with a few clicks. PRTG will be up and running in a just a few minutes including a first auto-configuration. [Smart Setup](#)^[52], the built-in interactive guidance dialog, will lead you through the whole process.

What is PRTG for?



- Monitoring and alerting you to up and downtimes or slow servers
- System health monitoring of your various hardware devices
- Network device monitoring, bandwidth accounting

- Application monitoring
- Monitoring virtual servers
- Service Level Agreement (SLA) monitoring
- System usage monitoring (for example, CPU loads, free memory, free disk space)
- Database performance and table values monitoring
- Email server monitoring and reviewing various backup solutions
- Monitoring your network's physical environment
- Classifying network traffic by source or destination, as well as content
- Discovering unusual, suspicious, or malicious activity with devices or users
- Measuring Quality of Service (QoS) and Voice over IP (VoIP) parameters
- Cloud monitoring services
- Discovering and evaluating network devices
- Collecting system information for various hardware types
- Finding unexpected relationships between your network components to detect potential security issues and assessing the real usage of your network and hardware
- Fail-safe monitoring using a failover cluster setup

What is Included in PRTG?

The PRTG on premises installer or a PRTG hosted by Paessler instance contains everything necessary to run your monitoring system immediately without any third-party modules.

- High performance: the fast and efficient database system that PRTG includes stores raw monitoring results, as well as logs, toplist, and tickets (outperforms SQL servers for monitoring data), accessible through the Application Programming Interface (API). You can distribute high loads on multiple probes.
- Low system requirements: For PRTG on premises an average PC (not older than 2 years) is sufficient and even a netbook can monitor over a thousand sensors. For detailed system requirements see [here](#)^[23]. PRTG hosted by Paessler does not even require any hardware for the PRTG core server!
- High security standards: SSL encryption for connections and web servers, a personalized user rights management, and much more.
- A built-in SSL-secured web server with HTTP and HTTPS support for the user interface.
- Fast web interface, works as Single Page Application (SPA) to avoid time-extensive reloading of pages.
- A built-in email relay server for automatic email delivery.
- Customizable, personalized alerting
 - Various notification technologies, for example, email, push, SMS text messages, syslog and SNMP traps, HTTP requests, event logs, Amazon SNS, executing scripts.

- Multiple triggers, for example, status alerts, limit alerts, threshold alerts, multiple condition alerts, escalation alerts.
- Gradual dependencies to avoid alarm floods, acknowledging certain alarms to avoid further notifications for this alarm, and alert scheduling.
- In-depth report generator to create reports on-the-fly as well as scheduled reports in HTML, PDF, and as CSV or XML data files. Several report templates are available by default.
- Graphics engine for user-friendly live and historic data graphs.
- Network analysis modules to automatically discover network devices and sensors.
- Distributed monitoring to monitor several networks in different locations.
- Special features for Managed Service Provider (MSP) to monitor customer networks and increase the quality of service.
- Data publishing with real-time dashboards—private and public—including live performance and status information. You can design these maps as you like with many different objects, as well as integrate external custom objects.
- Multiple languages such as English, German, Spanish, French, Portuguese, Dutch, Japanese, Russian, and Simplified Chinese.
- Customization: The PRTG Application Programming Interface (API) allows you to develop your own features. Additionally, you can create custom sensors, notifications, and device templates according to your specific requirements.

PRTG Network Monitor supports monitoring up to several thousand sensors per installation, depending on various parameters. It can optionally work with multiple remote probes to monitor multiple sites or network segments from one central core installation, and to distribute high monitoring loads. You can also configure fail-safe monitoring using a cluster installation to perform automatic failovers. Single failover installations are allowed with every PRTG license.

PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG hosted by Paessler. With PRTG on premises, the core server and local probe run within your network. PRTG hosted by Paessler is the PRTG cloud solution, where we at Paessler run the core server and hosted probe for you. The [PRTG web interface](#) for monitoring configuration and reviewing monitoring data is the same for both, PRTG hosted by Paessler and PRTG on premises.

The software is based on Paessler's reliable monitoring technology that has been constantly improving since 1997. There are already more than 200,000 PRTG installations running all over the world. Our outstanding [support](#) ensures your inquiries are answered within one business day for best possible network monitoring. Attractive licensing packages from freeware (up to 100 sensors) to enterprise level (with thousands of sensors) and the free choice between PRTG on premises and PRTG hosted by Paessler make sure every user finds the best-possible solution.

1.3 New in This Version

Our **continuous development and rollout** constantly improves and expands the functionalities provided by PRTG. Instead of delivering only a few versions each year with massive changes in every update, PRTG is automatically and seamlessly enhanced with new features and fixes—fast and with high quality.

We provide three release channels for PRTG on premises:

- **Stable:** Best tested version of PRTG for live systems. It is updated about once or twice a month and for use on live systems.
- **Preview:** Offers the latest features and fixes and is updated several times a month. Consider this version as "beta", so **do not use** this version on live systems you depend on!
- **Canary:** Providing "nightly builds" and is updated very often. It is not tested extensively. **Never use** on live systems you depend on!

Via these three channels, you can choose either maximum stability, early access to new features, or a mix of both.

 PRTG hosted by Paessler does not have release channels. Instead, we roll out the latest Stable version to PRTG hosted by Paessler instances in stages.

 For an overview of all recent changes in the current version, visit the [release notes for the stable release channel](#) on our website.

More

Paessler Website: Release Notes for the "Stable" Release Channel

- <https://www.paessler.com/prtg/history/stable>

Paessler Website: PRTG Network Monitor Version History

- <https://www.paessler.com/prtg/history>

Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

- <https://www.paessler.com/blog/prtg-12-introduces-continuous-rollout>

1.4 Available Licenses

Our licenses count by sensors. We define one sensor as one aspect that you monitor on a device.

There are three different PRTG flavors available.

Freeware Edition

The Freeware Edition is a good solution to get started with PRTG or for private use:

- Free for personal and commercial use.
- Can monitor up to 100 sensors.
- Supports all available sensor types.

 If you want to use the Freeware Edition, please first install the [Trial Edition](#)^[21] and get a free trial key. After the trial period has ended, your Trial Edition automatically turns into a Freeware Edition.

 This option is not available in PRTG hosted by Paessler.

Trial Edition

The Trial Edition is intended for evaluation purposes for customers who are interested in purchasing commercial licenses:

- Can monitor an unlimited number of sensors.
- Supports all available sensor types.
- For PRTG on premises you have to request the temporary license key from our website. Usually you see the license details including the key if you click the free download button on paessler.com
- The trial period of PRTG on premises is limited to 30 days and automatically reverts to [Freeware Edition](#)^[21] afterwards.
- PRTG hosted by Paessler provides a 10 days trial. Afterwards, your instance will be deleted if you do not purchase a commercial edition.
- Each PRTG on premises license includes one single failover [cluster setup](#)^[130], consisting of two nodes. Cluster installations with two and three failover nodes will require one additional trial license key. A cluster installation with four failover nodes will require two additional trial license keys.

After the trial period has ended, a PRTG on premises Trial Edition automatically turns into a Freeware Edition, allowing you to monitor up to 100 sensors for free.

Commercial Editions

There are several licenses of PRTG Network Monitor available to suit the demands of smaller as well as larger customers and organizations:

- Can monitor a maximum number of sensors (please consider our [recommendations](#)^[28]).
- Supports all available sensor types.
- Each PRTG on premises license includes one single failover [cluster setup](#)^[130], consisting of two nodes. Cluster installations with two and three failover nodes will require one additional license of the same size. A cluster installation with four failover nodes will require two additional licenses of the same size.

 For more information about available commercial licenses, please see the Paessler FAQs: [What is the difference between the PRTG Network Monitor licenses?](#)

More

Paessler Website: Get a Free PRTG Trial Key and Download PRTG for Evaluation

- <https://www.paessler.com/prtg/trial>

Paessler FAQs: What is the difference between the PRTG Network Monitor licenses?

- <https://www.paessler.com/support/faqs#e1912>

1.5 System Requirements

PRTG Network Monitor consists of two main system parts, the PRTG core server and one or more probes.  For details, see section [Architecture and User Interfaces](#) ^[125].

- If you want to use PRTG on premises, you need to install the PRTG server on a computer that meets the [System Requirements for PRTG Core Server \(PRTG on Premises\)](#) ^[23].
- If you want to use PRTG hosted by Paessler, you need to install at least one remote probe on a computer that meets the [System Requirements for PRTG Remote Probes](#) ^[23].

System Requirements for PRTG Core Server (PRTG on Premises)

To install a PRTG on premises server and work with it, you need to meet the following requirements:

- A current PC or server with at least a dual core CPU and a minimum of 2048 MB RAM memory is sufficient for the PRTG server.
- We recommend that you use the operating system **Microsoft Windows Server 2012 R2** for best performance.
- A web browser to access the web interface. The following browsers are officially supported:
 - Google Chrome 67 or later (recommended)
 - Mozilla Firefox 61 or later
 - Microsoft Internet Explorer 11

 PRTG hosted by Paessler does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG hosted by Paessler.

System Requirements for PRTG Remote Probes

- **Hardware**
A current PC or server with at least a dual core CPU and a minimum of 2048 MB RAM memory is sufficient for remote probes.
- **Operating system**
We recommend that you use the operating system **Microsoft Windows Server 2012 R2** for best performance. Microsoft Windows 10 and Windows Server 2016 are also good options for remote probes.
- **Stable network connection**
Remote probes require a stable network connection between the PRTG server and the remote probe. Remote probes that connect to a PRTG hosted by Paessler server need a reliable internet connection. Unstable connections, for example via 3G, might work but it is possible that you lose monitoring data if the connection is non-reliable.

 Why are remote probes helpful for monitoring with PRTG? Because you can extend your monitoring.

- Remote probes allow you to monitor different sub-networks that are separated by a firewall from your PRTG on premises core server and to keep an eye on remote locations. You can install [one or more remote probes](#)^[3708].
- Remote probes are useful if you want to distribute monitoring load by taking it from the system running the PRTG core server and putting it on one or more remote probe machines.
- You will need a remote probe if you want to monitor your local network using a PRTG hosted by Paessler instance.
- Remote probes may be suitable monitoring components in several individual scenarios that depend on your custom network setup.

Planning a PRTG on Premises Installation With Hundreds of Sensors or More?

The maximum number of sensors you can monitor with one PRTG on premises installation mainly depends on the monitoring technology and the monitoring intervals you use. In general, we recommend that you use a dedicated physical machine to run both the PRTG core server and PRTG remote probes.

 For more information, see section [Detailed System Requirements](#)^[26].

 PRTG hosted by Paessler is restricted to max. 5,000 sensors, more sensors are not possible. This number of sensors is available in the PRTG-5000 subscription.

More

- [Update From Previous Versions](#)^[83]

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- <https://www.paessler.com/prtg/requirements>

Knowledge Base: Planning Large Installations of PRTG Network Monitor

- <https://kb.paessler.com/en/topic/26383>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Knowledge Base: Checklist for Running PRTG on VMware

- <https://kb.paessler.com/en/topic/49193>

Knowledge Base: Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update, Activation, etc.?

- <https://kb.paessler.com/en/topic/32513>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

PRTG hosted by Paessler: Enter a New Era of Monitoring

- <https://my-prtg.com>

1.5.1 Detailed System Requirements

This section shows different aspects of system requirements for PRTG. Please consider these requirements to avoid issues while monitoring your network.

- [Supported Operating Systems](#) ^[26]
- [Hardware Requirements](#) ^[27]
- [Network Size: Recommendations](#) ^[28]
- [Running PRTG on Virtual Machines](#) ^[30]
- [Running PRTG in a Failover Cluster](#) ^[30]
- [Web Browser Requirements](#) ^[31]
- [Screen Resolution](#) ^[31]
- [Requirements for Monitored Devices](#) ^[31]
- [Requirements for the Enterprise Console](#) ^[32]
- [Requirements for Smartphones](#) ^[32]
- [More](#) ^[32]

 PRTG hosted by Paessler does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG hosted by Paessler.

Supported Operating Systems for PRTG Server and Remote Probes

The 32-bit and 64-bit versions of the following operating systems are officially supported for PRTG **Core Service** and **Probe Service**:

- Microsoft Windows Server 2012 R2* (recommended)
- Microsoft Windows Server 2016*
- Microsoft Windows Server 2012*
- Microsoft Windows 10**
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2*

* Windows servers in **Core** mode or **Minimal Server Interface** are not officially supported.

** The PRTG Enterprise Console is not fully compatible with Windows 10.

The version (32-bit or 64-bit) of the PRTG Core Server depends on the version of your operating system. The 64-bit version of the PRTG Core Server will be installed if

- the operating system is a 64-bit Windows system, **and**

- the system provides 6 GB RAM or more.

Otherwise the 32-bit version of the PRTG Core Server will be installed.

- For best performance of VMware sensors, EXE/Script sensors, and some other sensor types, we recommend Windows Server 2012 R2 on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#).
- For best performance of hybrid sensors using Windows Performance Counters and Windows Management Instrumentation (WMI), we recommend Windows 2008 R2 or higher on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#).
- **Microsoft .NET Framework:** We recommend that you provide Microsoft .NET Framework versions 4.5 or later (with latest updates) on all systems running a PRTG probe. The .NET framework is imperatively needed for monitoring VMware and XenServer virtual environments. Also some other sensor types need the Microsoft .NET Framework to be installed on the computer running the PRTG probe. This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#). Required versions are 4.5, 4.6, or 4.7. For details, see the Knowledge Base: [Which .NET version does PRTG require?](#)
- **Disabled FIPS Mode:** Ensure the **FIPS (Federal Information Processing Standards)** mode (Windows security option "System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.") is disabled on Windows systems running the PRTG core or probe service. FIPS-compliant encryption may cause errors of sensors which use the .NET framework. For details, see the Knowledge Base: [Why should I disable the FIPS mode under Windows?](#)

Hardware Requirements for PRTG Server and Remote Probes

Hardware requirements for PRTG **Core Service** and **Probe Service** mainly depend on the sensor types and intervals used. The following values are provided as reference for common usage scenarios of PRTG (based on a default sensor interval of 60 seconds).

- **CPU**
A current PC or server with at least a dual core CPU can easily monitor up to 2,000 sensors (see sensor type specific notes below). PRTG supports native x86/x64 architectures.
- **RAM memory**
Minimum requirement: 2048 MB RAM. You need about 150 KB of RAM per sensor.
- In general, we recommend at least 1 additional CPU core and 1 GB RAM per additional 1,000 sensors.
- **Hard Disk Drive**
You need about 200 KB of disk space per sensor per day (for sensors with 60 second interval).
- **Internet connection**
An internet connection is required for license activation (via HTTP or email).
- **Stable network connection for remote probes**
Remote probes require a stable network connection between the PRTG core server and the remote probe. Unstable connections, for example via 3G, might work but it could be possible that you lose monitoring data if the connection is non-reliable.

There are also non-hardware dependent limitations for some sensor types, for example, WMI and SNMP V3 sensors. These limitations can be overcome by distributing the sensors across multiple [remote probes](#)³⁷⁰⁷. For clusters we recommend that you stay below 2,500 sensors per cluster.

 It is crucial for a properly working PRTG server to have a certain amount of hardware resources available. If the server runs out of resources, PRTG will send warning and emergency messages to the primary email address of the **PRTG System Administrator** user. You will receive **warning** messages if available disk space falls below **1 GB** or memory below **500 MB**, and **emergency** messages if available disk space or memory falls below **50 MB**. Please react immediately and free system resources!

Network Size: Recommendations

- Rule of thumb: Typical PRTG installations almost never run into performance issues when they stay under 5,000 sensors, under 30 remote probes, and under 30 user accounts.
- PRTG can scale much higher if the installation is well planned. Please read on if you plan to go beyond these numbers and/or if you plan elevated use of resource intensive features like reporting, xFlow sensors, or clustering.
- If you plan an installation that monitors more than 10,000 sensors from one instance of PRTG on a physical device or more than 5,000 sensors with PRTG running on a virtual machine we ask you to [contact your presales team](#) for consultation.
- To give you an impression: To monitor 5,000 sensors in a 1-minute interval, PRTG takes 7.2 million measurements and evaluates, notifies, and stores them—this adds 700 MB of additional data to the database every single day.

 PRTG hosted by Paessler is restricted to max. 5,000 sensors, more sensors are not possible. This number of sensors is available in the PRTG-5000 subscription.

Apart from the processing power required for the monitoring itself, several aspects can affect the number of sensors that you can use with PRTG. The following recommendations are for a PRTG single core setup (without clustering) on a physical machine. You can overcome some of these limitations if you distribute the sensors across multiple remote probes.

SIZE RECOMMENDATIONS

Operating System	We recommend that you use Windows Server 2012 R2 to run the PRTG core server and probes. This offers superior performance for monitoring, especially if you have more than 2,000 sensors.
Sensor Types	Ping ¹⁵²⁹ and SNMP sensors ⁴³¹ create much less load than complex sensors like xFlow sensors ³⁵¹⁴ , VMware sensors ⁴³⁵ , Sensor Factory sensors ¹⁷²⁰ , WMI sensors ⁴³³ , or Syslog ²⁶⁵⁶ / Trap receiver ²⁴⁷⁹ sensors, for example.
Scanning Interval	We recommend that you mainly use 1-minute scanning intervals ³⁴⁵ for up to 2,000 sensors and 5-minute intervals if you have more sensors.

SIZE RECOMMENDATIONS

Number of Users	We recommend that you stay below 30 active user accounts for each PRTG core server. You can work well with more users if these do not all use the user interfaces at the same time (including public dashboards).
Number of Remote Probes	Our general recommendation is to stay below 30 remote probes on one PRTG core server. PRTG still scales well up to 60 probes as long as you have less than 100 sensors per probe.
CPU Intensive Features	Try keeping the usage of the following features down: Many quickly refreshed dashboards , frequent generation of huge sensor reports , heavy usage of packet sniffing , factory sensors , and toplists , frequent automatically scheduled auto-discoveries for large network segments, constant queries of monitoring data via the API , among others.
Network Connection Quality	The quality of your network also plays an important role. When monitoring via UDP, for example, a high packet loss rate can lead to frequent timeouts. Remote probes that connect via unstable (WAN) connections can lead to delays as well.

In general, consider the following rules for the performance impact of different sensor types:

- **SNMP V1 and V2, Ping, Port, and HTTP**
We recommend that you use these sensor types for scenarios with thousands of sensors.
- **SNMP V3**
You can monitor about 5,000 SNMP V3 sensors with an interval of 60 seconds on a common two core computer, and about 10,000 sensors on a four core system (the main limiting factor is your CPU power).
- **WMI**
Try to keep the number of WMI sensors per probe below 120 sensors (with 60s interval), or 600 sensors (with 300s interval).
- **xFlow (IPFIX, NetFlow, sFlow, jFlow)**
Monitoring the maximum number of sensors depends on the traffic pattern, the number of xFlow packets per second received by the PRTG probe, as well as the performance of the probe system.
- **Packet Sniffer**
These sensors create the highest CPU load on the probe system. This technology is only recommended for monitoring of low traffic connections (<50 Mbit/s steady stream). When traffic is often over 10 Mbit/s a dedicated remote probe should be used.
- **VMware Monitoring**
Monitoring of VMware is limited to about 20 sensors at a 60 seconds monitoring interval, or 100 sensors at a 5 minutes interval. On probes running on Windows Server 2012 R2, you can use more VMware sensors. These limitations issue from the VMware platform. For details, see this Knowledge Base article: [Increasing Maximum Connections for VMware sensors](#)

▪ Other sensor types

The impact of a specific sensor type on performance is indicated by a color range when adding a sensor to a device. It ranges from dark green (very low impact) to bold red (very high impact).

To overcome any limitations mentioned above you should distribute the sensors over two [remote probes](#)³⁷⁰⁹ or more.

Running PRTG on Virtual Machines

You can run the PRTG core server as well as PRTG remote probes on virtualized platforms. However, we strongly recommend that you use a dedicated physical machine to run the PRTG core server or the [PRTG remote probes](#)³⁷⁰⁹.

There are several reasons why we recommend that you run PRTG (core server and remote probes) on real hardware, especially for thousands of sensors. Each sensor request will have to go through many virtualization layers, which costs performance and makes measurements less exact. In our experience, a physical machine simply works best for a thousand sensors and more.

Our recommendation to use real hardware is valid for the PRTG core server and for remote probes. If you must run PRTG on a virtual machine, please stay below 5,000 sensors per virtual machine and consider running several PRTG core server instances instead.

 We cannot offer technical support regarding performance and stability problems for PRTG installations on virtual machines that run with more than 5,000 sensors. In this case, please migrate PRTG to one or more, preferably physical, machines.

 When running PRTG on a virtual machine, do **not** use dynamic resource allocation, but please make sure that full resources are available to the virtual machine at any time. In our experience, dynamic resource allocation is not working efficiently for a monitoring software and can lead to massive performance issues. Do not distribute CPU cores over different CPU sockets in your VM configuration. Scheduling threads does not work properly in this case, which results in performance issues.

 For more details, see this Knowledge Base article: [Checklist for Running PRTG on VMware](#)

Running PRTG in a Failover Cluster

We recommend a single [failover setup](#)¹³⁰ if you need fail-safe monitoring. This consists of two PRTG core servers, each working as a cluster node.

In a PRTG failover cluster, the monitoring load doubles with each cluster node, so you will encounter half performance for each additional cluster node. In a single failover cluster, please divide our recommended numbers from above in half.

 This feature is not available in PRTG hosted by Paessler.

Web Browser Requirements

The following browsers are officially supported by the PRTG web interface (in order of performance and reliability):

- Google Chrome 67 or later (recommended)
- Mozilla Firefox 61 or later
- Microsoft Internet Explorer 11

For security and performance reasons, we strongly recommend that you always use the latest version of Google Chrome to access the PRTG web interface.

- ❗ Firefox is potentially vulnerable for **cross-site scripting (XSS)** attacks. These XSS exploits are possible if you click **phishing** links that contain malicious code, for example, in emails, and you are currently logged in to PRTG with Firefox. For more information, see this Knowledge Base article: [How secure is it to access the PRTG web interface with Firefox?](#)
- ❗ Microsoft Internet Explorer 11 and Microsoft Edge, as well as other current browsers that are not officially supported have issues with some functionalities of the PRTG web interface. However, you can access the web interface with any browser.
- ❗ Deprecated Internet Explorer versions as well as some mobile browsers might not be able to display the fully featured [Ajax web interface](#)^[166].
- ❗ Plugins may have an effect when viewing the PRTG web interface. Please make sure to add exceptions for PRTG in the plugins' settings, especially when using ad blockers. See also this Knowledge Base article: [The logs page in the PRTG web interface does not load. What can I do?](#)

Screen Resolution

A screen resolution of at least 1024x768 pixels is sufficient for most functions of PRTG. However, we recommend a screen resolution of 1200x800 or higher.

Requirements for Monitored Devices

- **SNMP monitoring**
The monitored device(s) must be equipped with SNMP Version 1, 2c, or 3 (an SNMP-compatible software must be installed on the device). SNMP must be enabled on the device and the machine running PRTG must be granted access to the SNMP interface. For details, see section [Monitoring via SNMP](#)^[3489].
- **Windows/WMI monitoring**
To use Windows Management Instrumentation (WMI) monitoring, you need a Windows network. For client PCs monitored with WMI, only the [operating systems as given above](#)^[26] are officially supported, but do not use Windows 2008 for WMI monitoring (strong performance issues). For details, see section [Monitoring via WMI](#)^[3507].

- **xFlow (IPFIX, NetFlow, sFlow) monitoring**
The device must be configured to send NetFlow data packets (NetFlow version 5, 9, or IPFIX) or sFlow packets (version 5) to the machine running the PRTG probe. For details, see section [Monitoring Bandwidth via Flows](#)^[3514].
- **Packet Sniffer monitoring**
Only data packets passing the local machine's network card can be analyzed. Switches with so-called 'monitoring ports' are necessary for network-wide monitoring in switched networks. For details, see section [Monitoring Bandwidth via Packet Sniffing](#)^[3512].
- **Other sensor types**
Depending on the specific sensor type, you can find requirements (for example, modules, components, device configurations) that may have to be fulfilled in the corresponding manual section, as well as when adding the sensor to a device.

Requirements for the Enterprise Console

The optional PRTG [Enterprise Console](#)^[3430] (EC) runs under all [supported Windows versions](#)^[26], but it is not fully compatible with Windows 10. Running the EC on Windows 10 results in several issues so please use another operating system. We will consider full Windows 10 support for future PRTG desktop clients.

 PRTG hosted by Paessler does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

The EC has a built-in webkit browser engine and requires no specific browser installed on the system. See also [Enterprise Console—Requirements for Connections to PRTG Web Server \(s\)](#)^[3431].

Requirements for Smartphones and Tablets

PRTG supports optional mobile apps for iOS and Android devices.

 For more information and system requirements, see section [PRTG Apps for Mobile Network Monitoring](#)^[3484].

More

- [Update From Previous Versions](#)^[83]

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- <https://www.paessler.com/prtg/requirements>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Knowledge Base: My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Knowledge Base: Frequent Questions about xFlow, Packet Sniffing, Traffic Monitoring and Cisco

- <https://kb.paessler.com/en/topic/3733>

Knowledge Base: Increasing Maximum Connections for VMware Sensors

- <https://kb.paessler.com/en/topic/30643>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Checklist for Running PRTG on VMware

- <https://kb.paessler.com/en/topic/49193>

Knowledge Base: Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Knowledge Base: How secure is it to access the PRTG web interface with Firefox?

- <https://kb.paessler.com/en/topic/70192>

Knowledge Base: Why should I disable the FIPS mode under Windows?

- <https://kb.paessler.com/en/topic/71305>

1.6 Introduction: Monitoring with PRTG

This manual section provides an overview of basic principles of PRTG Network Monitor. It shows you how you can prepare your IT infrastructure for monitoring with PRTG. Of course, you do not have to re-configure your whole network for PRTG, but there are several topics that are useful to consider before actually using PRTG.

You can immediately start monitoring without complicated configuration steps. See the [Quick Start Guide](#) for details. If you want to know more details right from the beginning, read through the manual section below. It covers these topics:

- [Overview](#)
- [What PRTG Does](#)
- [Where to Install PRTG](#)
- [How to Monitor](#)
- [What can PRTG Monitor](#)
- [How to Prepare](#)
- [What Hardware Do I Want to Monitor](#)
- [Types of Logins and Credentials](#)
- [Monitoring Technologies](#)
- [Notifications from PRTG](#)
- [Advanced Topics](#)

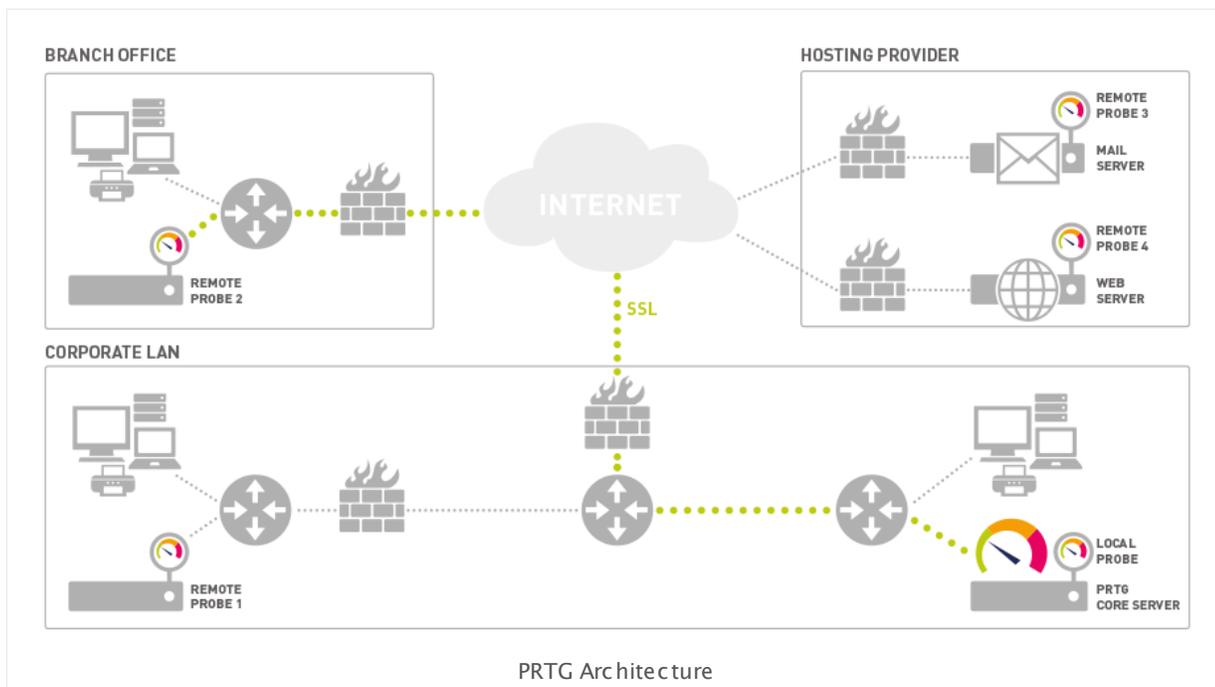
Overview

PRTG Network Monitor is a monitoring software that is flexible and easy to use. You can [download, install, and configure](#) PRTG on premises or [create a PRTG hosted by Paessler instance](#) within minutes and start monitoring right away.

That said, you will not immediately have full access to all relevant information unless your network is completely ready for monitoring—for example, PRTG needs credentials to access devices in your network. During the PRTG on premises install process, PRTG will automatically add devices with some default sensors, such as the [Ping sensor](#). But it will only add devices and sensors where no credentials or certain technologies are needed. For PRTG hosted by Paessler you will need to install a remote probe in your LAN first to monitor your network.

What PRTG Does

PRTG is a **Unified Monitoring Tool** that allows you to monitor pretty much anything with an IP address. PRTG consists of a [core server](#) which is responsible, for example, for the configuration, data management, and web server, and one or more [probes](#) (local or hosted, [remote](#)), which perform data collection and monitoring processes on [devices](#) via [sensors](#).



Sensors are the basic building blocks of PRTG and are organized in an [Object Hierarchy](#)¹³³. A sensor can tell you about one or more aspects (referred to as [channels](#)¹³⁶) of a device or node. For example:

- Uptime
- Load
- Interface throughput
- Bandwidth usage (for example, flows)
- Loading times
- Speed
- Hardware status
- Temperature
- Quality
- Resource consumption
- User counts
- Record counts
- Log events
- Database requests

Where to Install PRTG

For best performance, we will always recommend that you install PRTG on premises on a physical machine. Any current PC or server with at least a dual core CPU and 2048 MB RAM will suffice for most average installations. PRTG can also run on a virtual machine (VM), but we have a [recommended limit](#)^[30] on the number of sensors due to the hypervisor overhead.

For remote sites and for offloading work, you can use the [PRTG Remote Probe](#)^[3709]. Remote probes offer a smaller footprint data collector that reports back to the PRTG core server and so helps minimize performance impacts. At least one remote probe is required for PRTG hosted by Paessler to monitor your local network.

 PRTG hosted by Paessler does not require any hardware for the PRTG server, but at least one remote probe installation is necessary to monitor your local network when using PRTG hosted by Paessler.

How to Monitor

There are the following ways for PRTG to receive monitoring data from target devices:

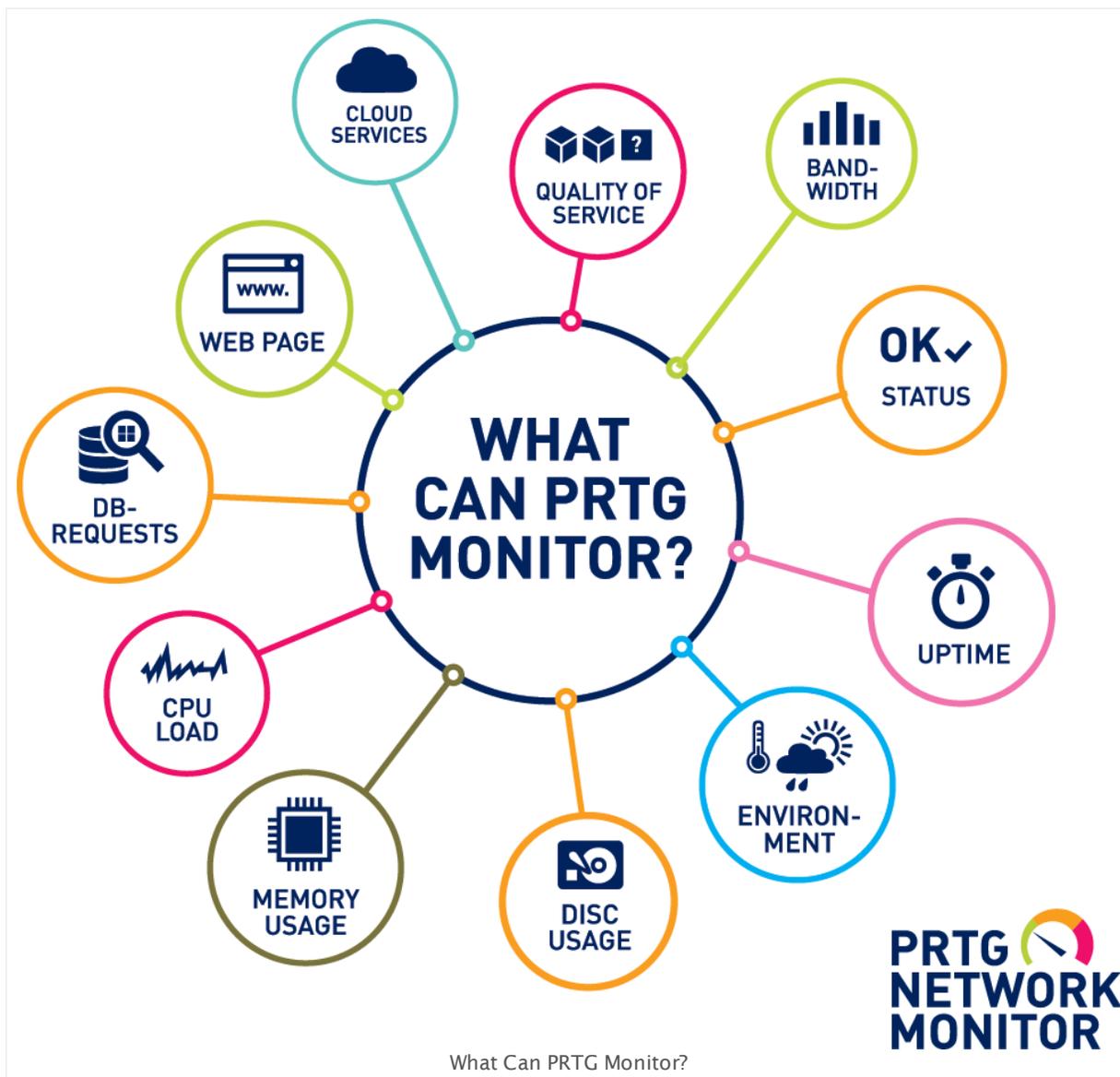
- Polling or querying sensor data: PRTG actively obtains data from a device and refreshes it in regular intervals. This includes, for example, device status, resource usage, and performance metrics. Most sensor types use this method. PRTG can also consume and collect sensor data based on interface with, for example, HTTP(S) requests, port checks, email checks, FTP downloads, and database requests.
- Listening or receiving sensor data: PRTG passively receives data that is pushed to PRTG by a device or application. This includes, for example, unexpected events, Syslogs and SNMP traps, detailed data flow (bandwidth monitoring), and event log messages.

Most of the monitoring data that PRTG collects is actively queried. It is the basis for statistical sampling to see how a device or application is performing over time. For more information, see section [Monitoring Technologies](#)^[39] below.

What Can PRTG Monitor

Out of the box, PRTG comes with more than [200 different sensor types](#)^[429] ranging from specific platform sensors over generic hardware and bandwidth sensors to custom scripts. Specific sensors that are pre-configured for common configurations allow you to quickly gather the information you need. Just add these sensors to the target devices they are designed for and receive monitoring data instantly.

Additionally, PRTG provides the possibility to add custom sensors. For example, you can create individual sensors for devices that PRTG does not provide sensor types for out of the box, or write scripts that return data from some application. See also the [PRTG Script World](#) for custom sensors that are ready to use.



How to Prepare

Best practice for the first step in good monitoring is to make a plan. Think about the following questions.

1. What needs to be monitored in my IT infrastructure?
2. How can I retrieve the needed information? Which technologies and credentials are required?
3. Which notification methods do I want to use to get alerted if there is something wrong?

You can take the following sections as a basis for your monitoring planning.

What Hardware Do I Want to Monitor

When choosing what to monitor, we recommend that you add the most important devices within your infrastructure first. Start with the core network and other infrastructure that all network devices depend upon, your **Business Critical Tier-1**. This usually includes key infrastructure such as core routers, switches, Virtual Private Network (VPN), firewalls, and basic network services such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and authentication like Lightweight Directory Access Protocol (LDAP).

As an example, if you are a web business, your web infrastructure is absolutely critical. You will want to add devices in order of importance to your business: file services, databases, and other systems. Usually, you would monitor devices from several perspectives, like hardware health, service availability, and performance.

 See also our video tutorial on [webserver monitoring](#).

Hardware Overview

There is a huge number of different vendors with uncountable variations of hardware devices, so hardware details go beyond the scope of this article. Every IT infrastructure is individual, but here are the main points you should consider.

1. Core infrastructure
 - a. Routers, switches, firewalls
 - b. Core network services: DNS, Active Directory, LDAP servers
2. For your hardware devices, you need statistics on availability, usage, and performance.
3. PRTG will retrieve data using standard protocols:
 - a. Ping, Simple Network Management Protocol (SNMP); web queries via HTTP and HTTPS; email via Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP)
 - b. Hardware parameters via SNMP, SSH, Simple Object Access Protocol (SOAP)
 - c. Bandwidth usage via xFlow (NetFlow, IPFIX, sFlow, jFlow), packet sniffing, SNMP
 - d. Windows systems via Windows Management Instrumentation (WMI)
 - e. Other interfaces via Secure Shell (SSH) and scripts (for example, PowerShell and Python)

PRTG will monitor, track, and chart data, as well as generate alarms.

Types of Logins and Credentials

Many of the sensors included in PRTG rely on access through logins to specific systems. You will need different credentials with sufficient permission for all the different devices, operating systems, and domains. The configuration may also be different if you want PRTG to act as a Syslog or SNMP trap receiver or for tracking flows.

In most cases, PRTG will use the following credential types to access the devices that you want to monitor.

- SNMP credentials
- Windows credentials (WMI)
- Linux, Solaris, and macOS credentials (SSH/WBEM)
- VMware and XenServer credentials
- Database Management Systems (DBMS) credentials
- Other credentials (for example, Amazon CloudWatch keys, HTTP proxy)

Define your (administrative) credentials for all types of target devices that you want to monitor in the **Root** group of the device tree. Devices that you add to PRTG will [inherit](#)¹³⁷ these automatically, so often you will not have to re-enter credentials, depending on the used monitoring technology.

Monitoring Technologies

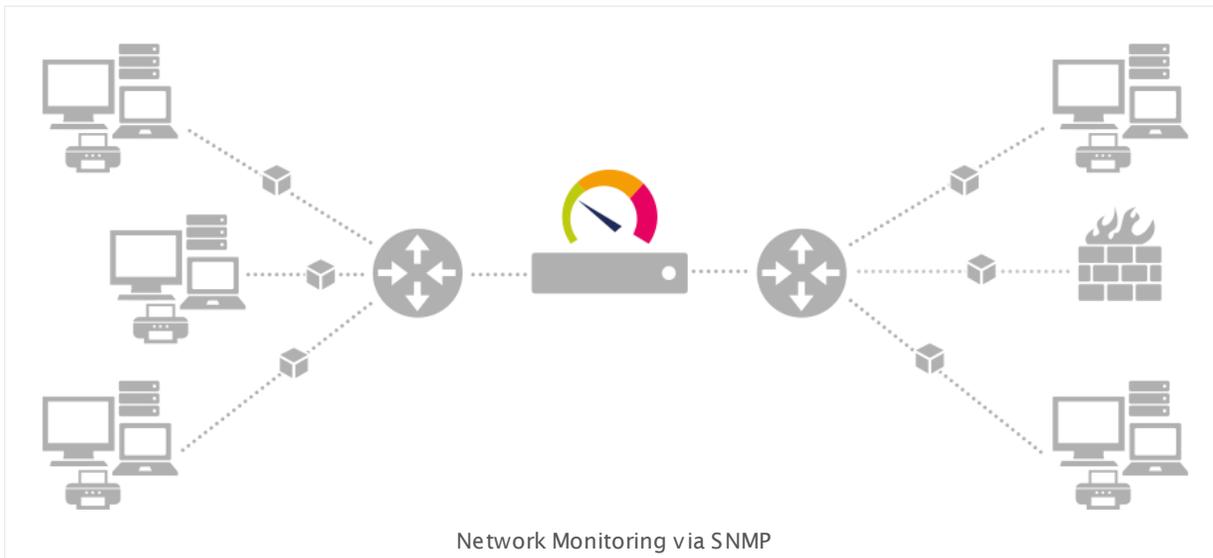
This section briefly describes the most common monitoring technologies.

 For details, see manual section [Sensor Technologies](#)³⁴⁸.

Monitoring with Simple Network Management Protocol (SNMP)

SNMP is a set of standards for communication with devices in a TCP/IP network. SNMP monitoring is useful if you are responsible for servers and network devices such as hosts, routers, hubs, and switches. It enables you to keep an eye on network and bandwidth usage, and monitor important issues such as uptime and traffic levels.

You can use SNMP to monitor the bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory and CPU load. The target devices must support SNMP. Most devices with enabled SNMP require the same configuration like SNMP version and community string. To find out how to set up SNMP on a specific device, search in the internet for your device name or model and SNMP configuration. You will likely get plenty of information on how to configure SNMP.



When you use a sensor with this technology, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These queries trigger reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Con: Limited security because it only uses a simple password ([community string](#)³⁴⁹²) and sends data in clear text (unencrypted). Because of this, you should only use it inside LANs behind firewalls, but not in WANs. Version 1 only supports 32-bit counters, which are not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.
- Con: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.

- Con: Difficult to configure and higher overhead for the probe, which will reduce the number of devices that you can monitor (see [here](#)^[3491] for more information).

SNMP Traps

Various devices can send SNMP trap messages to notify you of system events.

- PRTG supports SNMP v1 and SNMP v2c traps.
- Destination for SNMP traps: IP address of the trap receiver, which is the IP of the PRTG probe system (server with either a local or remote probe running on it) to which you add the [SNMP Trap Receiver Sensor](#)^[2479].

Which SNMP Version Should I Choose?

The SNMP version to choose depends on your environment, but as a guideline:

- If your network is publicly accessible, you may want to use SNMP v3, which has encryption and secure access. However security and encryption adds overhead, which results in less performance.
- If your network is isolated or well protected behind firewalls, the lower security of SNMP v1 or SNMP v2c may be sufficient.
- From the PRTG perspective, if you have a lot of devices to monitor, the SNMP v2c is preferable. It will allow you to monitor more devices on a shorter monitoring interval and supports 64-bit counters.

The most important thing is to set the same SNMP version in the PRTG settings (for example, on **Root** level) as you have configured in your target device. If you select an SNMP version that is not supported by the server or device you want to monitor, you receive an error message. Unfortunately, in most cases, these error messages do not explicitly point to the possibility that you use the incorrect SNMP version. These messages provide minimum information only, such as **cannot connect** or similar. Similar errors occur when community strings, usernames, or passwords do not match.

 For basic requirements for SNMP monitoring, see this Knowledge Base article: [My SNMP sensors don't work. What can I do?](#)

Monitoring Windows Systems

You can monitor Windows systems via [Windows Management Instrumentation \(WMI\)](#)^[3507] and [Windows Performance Counters](#)^[3509]. WMI is the Microsoft base technology for monitoring and managing Windows-based systems. PRTG uses this technology to access data of various Windows configuration parameters and status values. However, sensors using the WMI protocol generally have a high impact on system performance. In addition to strict WMI sensors, there are sensors that can use Performance Counters to monitor Windows systems.

To monitor via WMI and Performance Counters, it is usually sufficient to provide **Credentials for Windows Systems** in PRTG. However, monitoring via WMI is not always trivial and often causes issues.

 See this article in our Knowledge Base if you run into issues: [My WMI sensors don't work. What can I do?](#)

It is also possible to use Simple Network Management Protocol (SNMP) for Windows devices. The same information is often available using any of these protocols. From a performance perspective, the preference would be SNMP, and then WMI or Performance Counters.

Bandwidth and Traffic Monitoring: Flows and Packet Sniffing

Using flow protocols, you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view [Toplists](#) for all xFlow (NetFlow, IPFIX, sFlow, jFlow) sensors.

Flows are a type of monitoring data pushed from network devices to PRTG. You can use it to monitor where data is traveling to and from, and how much. This way it determines which machine, protocol, and user is consuming bandwidth. PRTG currently supports the following flow types:

- NetFlow v5/v9 and IPFIX: Originally introduced by Cisco and supported by several vendors
- jFlow: Traffic sampling technology introduced by Juniper networks
- sFlow: Short for sampled flow, introduced by HP. sFlow uses statistical sampling of the traffic at defined intervals to achieve scalability for high volume interfaces.

You can also use [packet sniffing](#) for bandwidth monitoring if your hardware does not support any of these flow versions.

Monitoring Passively Received Data

PRTG provides the option to monitor passively received data. For this purpose, you can set up a device in a way that it automatically sends the data to PRTG. Specific sensor types can receive this data and alarm you based on your individual settings. For example, all Linux/Unix and most network devices support remote devices generating data that has to be configured on each device, and sending the messages to a [PRTG probe system](#). Usually, only the destination IP and port are required.

Examples of this monitoring technology are [HTTP Push](#) sensors, as well as [Syslog](#) and [SNMP Trap](#) receivers.

 For more information, see our tutorial videos about the [Syslog Receiver sensor](#) and the [SNMP Trap Receiver sensor](#).

Monitoring with Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is a standard application layer protocol and the basis for data communication in the internet. HTTP is a request-response method for client-server architectures, where the client sends a request and the server processes and responds to the request.

Monitoring via HTTP is useful if you want to monitor websites or web servers. It enables you to keep an eye on the availability and download times of a website or the performance statistics of a web server. There are also a lot of other possible use cases for HTTP sensors. For example, you can request any Application Programming Interface (API) that is reachable via HTTP and monitor returned values. This approach makes it possible to include almost any type of device or application into your monitoring.

Notifications from PRTG

PRTG can notify you in [various ways](#) if it detects that there is something wrong in your network. You can individually define in which case (for example, [based on thresholds](#) or [on sensor states](#)) and how you want to receive notifications from PRTG. The most common methods would be [email](#), [SMS text message](#), and [push notifications](#) to your smartphone which runs a [PRTG mobile app](#).

For your critical infrastructure it is best practice to set up two redundant notifications with different delivery methods (for example, email and SMS via a gateway).

 For more information about notifications, see our video tutorials [PRTG – Notifications](#) and [Use Cases for PRTG Notifications](#).

Email Notifications

The most common notification method is to send emails using a Simple Mail Transfer Protocol (SMTP) server built-in in PRTG. This means no SMTP server setup or configuration is required, but if you want to deliver through your email server, you will have to configure it in the [PRTG SMTP settings](#).

SMS Text Notifications

PRTG on premises can also notify you on your mobile phone. To [deliver SMS text notifications](#), you can select one of the SMS service providers that PRTG includes by default and use it with your credentials for this provider. Of course, you can also use any other service provider by defining a custom URL (look in your provider's documentation for the required format). You can also use an SMS gateway to receive messages even if your internet connection is down. See our Knowledge Base for a [list of third-party tools](#).

Push Notifications

PRTG can send push notifications to iOS and Android, when you run the according PRTG mobile app on your smartphone.

 See the article [How can I use push notifications with PRTG?](#) in our Knowledge Base for more details.

Advanced Topics

So, now that you are ready for monitoring with PRTG, enjoy having all important information about your IT infrastructure available at a glance. To dive deeper into network monitoring with PRTG we entrust you to have a look at our [video tutorials for advanced topics](#). Of course, you will also find all relevant information about network monitoring in the PRTG User Manual!

More

Video Tutorials: PRTG Basics

- <https://www.paessler.com/support/videos/prtg-basics>

Video Tutorial: Webserver Monitoring

- <https://www.paessler.com/support/videos/prtg-basics/webserver-monitoring>

Video Tutorial: SNMP Trap Receiver

- <https://www.paessler.com/support/videos/prtg-advanced/snmp-trap-receiver>

Video Tutorial: Syslog Receiver

- <https://www.paessler.com/support/videos/prtg-advanced/syslog-receiver>

Video Tutorial: PRTG – Notifications

- <https://www.paessler.com/support/videos/prtg-basics/notifications>

Video Tutorial: Use Cases for PRTG Notifications

- <https://www.paessler.com/support/videos/prtg-basics/notifications-use-cases>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- <https://kb.paessler.com/en/topic/393>

Knowledge Base: How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

Part 2

Quick Start Guide

2 Quick Start Guide

Welcome to PRTG Network Monitor! This section gives a quick start into PRTG, so you can start monitoring your network right away!

Setting up monitoring for your network is easy! You only need to download the PRTG installer from the Paessler website and run through the installation wizard, or set up a PRTG hosted by Paessler instance on <https://my-prtg.com> and install a remote probe in your LAN. Provide some information about your network in the [Smart Setup](#) and PRTG will start monitoring your network immediately without any further complicated stumbling blocks! Of course, later on, you can still adjust everything to your needs.

See the following quick steps.

Quick Start Guide—Topics

- [ONE—Download, Installation, and First Login](#) ⁴⁸
- [TWO—Smart Setup](#) ⁵²

2.1 ONE—Download, Installation, and First Login

We offer two options to monitor your network with PRTG Network Monitor: use PRTG on premises to run the PRTG in your network, use PRTG hosted by Paessler to run PRTG on a server that Paessler hosts for you.

- If you want to use PRTG on premises, just download it from our website and install it on a Windows computer.
- ☁ PRTG hosted by Paessler does not require a download or installation to set up the PRTG server, just create an instance on <https://my-prtg.com>
- 📺 For video tutorials with PRTG basics, see the [video sections on paessler.com](#).

Download PRTG on Premises

You can find the installer for PRTG on our website <https://www.paessler.com>. There you can also login to the Paessler shop to buy or upgrade your license, or to renew your maintenance.

- ☁ This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

PAESSLER
THE NETWORK MONITORING COMPANY

HOME PRODUCTS DOWNLOADS SHOP SUPPORT PARTNERS BLOG COMPANY LOGIN SEARCH

Home > Products > PRTG Network Monitor > Download

INSTALLATION OF PRTG TAKES LESS THAN 2 MINUTES!

Monitor your network now! No additional software is required. All you need is a Windows PC or VM.

Running PRTG in your network is quick&easy. After installation it will scan your network and the Auto-Discovery will create all the [sensors](#) that are required to monitor your network.

FREE TRIAL DOWNLOAD
No limitations for 30 days

FREEMWARE DOWNLOAD
Limited to 100 Sensors, Free Forever

Christine, Business Development Manager at Paessler

Version Number, File Size	Version 17.2.31.1977 (May 10th, 2017), 157 MB
Available Translations	English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, Russian and Simplified Chinese
Operating Systems	All Windows versions (Windows 7 or later, see System Requirements)
What's new?	See Version History/Release Notes
Already PRTG customer?	Please log in to our website to download the full version

Download PRTG Network Monitor

Downloading PRTG Network Monitor

Please download the latest publicly available program version from the Paessler website. Simultaneously, you will receive a trial key. Enter this license key during the installation of PRTG. If you have already purchased a commercial license, use your commercial key. Please log in to the Paessler website to find your license key,

- <https://www.paessler.com/prtg/download>
- <https://shop.paessler.com/accounts/login/>

Every freeware installation starts as a trial version that allows you to use an unlimited number of sensors for 30 days. After the trial period has expired, your installation automatically reverts to the freeware edition with 100 sensors. Please understand that customers with a commercial license get prioritized support.

To upgrade your running trial or freeware version to a commercial edition, please purchase a commercial license key on <https://shop.paessler.com> and enter this key on the [license page](#) ^[3414] in the PRTG web interface.

Updates are free to customers with an active maintenance contract. If you do not have an active maintenance contract, please log in to the Paessler shop to renew it or contact sales@paessler.com.

 Once installed, the PRTG [Software Auto-Update](#) ^[3407] will automatically download and install new software versions. This helps you keep PRTG up to date without manually installing new PRTG versions.

Install PRTG on Premises

Double-click the setup file on the computer that you want to use as PRTG server. Follow the installation wizard and install the software.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

At the end of the installation, PRTG opens a new browser window automatically. It connects to the PRTG web interface, shows the [device tree](#) ^[181], and starts the [setup assistant](#) ^[52]. Please load the web interface with one of the officially supported browsers:

- Google Chrome 67 or later (recommended),
- Mozilla Firefox 61 or later,
- Microsoft Internet Explorer 11

We recommend that you use Google Chrome to access the PRTG web interface. Firefox has security issues and Internet Explorer as well as Microsoft Edge and other current browsers might have issues with some functionalities. See [Detailed System Requirements](#) ^[31] for more details.

 Due to scripting incompatibilities, you might not be able to use all functionalities of the PRTG Ajax web interface with Internet Explorer 10 or earlier and other older browsers. If you cannot access the PRTG web interface, please open the URL of PRTG in another browser.

Create a PRTG hosted by Paessler Instance

PRTG hosted by Paessler runs in the cloud, so setting up the PRTG server does not require a download or installation.

- Open <https://my-prtg.com> with a browser.
- You can directly start a free trial from there: enter your desired domain name (between 4 and 60 characters) and click **Start Free Trial Now**. You can reach your PRTG hosted by Paessler instance with your browser under `<yourdomain>.my-prtg.com` later.
- A window where you have to sign in will appear. You can directly sign in using your Google, Facebook, Windows, or Amazon account (via **Auth0**). In this case, click the desired service and sign in with your credentials. Alternatively, you can register at my-prtg.com using dedicated credentials.
- After signing in, choose your subscription plan, for example, you can start with a free trial for 10 days. Click **Subscribe Now** and PRTG will create an instance for you.

As soon as your instance is ready, the PRTG web interface will open, show the device tree, and start the [smart setup](#)^[52]. You can also instantly monitor all servers, services, and devices that are publicly available via the internet.

Please make sure you load the web interface with one of the [supported browsers](#)^[31]. We recommend that you always use the latest version of Google Chrome.

Login

If everything works fine, the first thing you will see will not be the login screen, but the device tree. You only have to log in manually if you use a different browser.

PRTG Network Monitor

Login Name

Password

[Login](#)

[Download Client Software \(optional, for Windows, iOS, Android\)](#)
[Forgot password?](#) [Need Help?](#)



[Paessler Blog](#)

Learn, Workshop and Discuss: Why You Should Atte...
 Hands-on Workshops, Serverless Architecture and Webpack For the second time in a row, we decided to participate in the Nuremberg Web Week and to share our knowledge about modern web applications with the local developer scene. This

PRTG Podcast: How to Clean Up after WannaCry
 As a follow up to the first ever, recently released PRTG podcast (which, if you haven't listened to already, you may need to re-assess your life choices - click here immediately!), Rupert Collier, our resident UK sales manager and aspiring

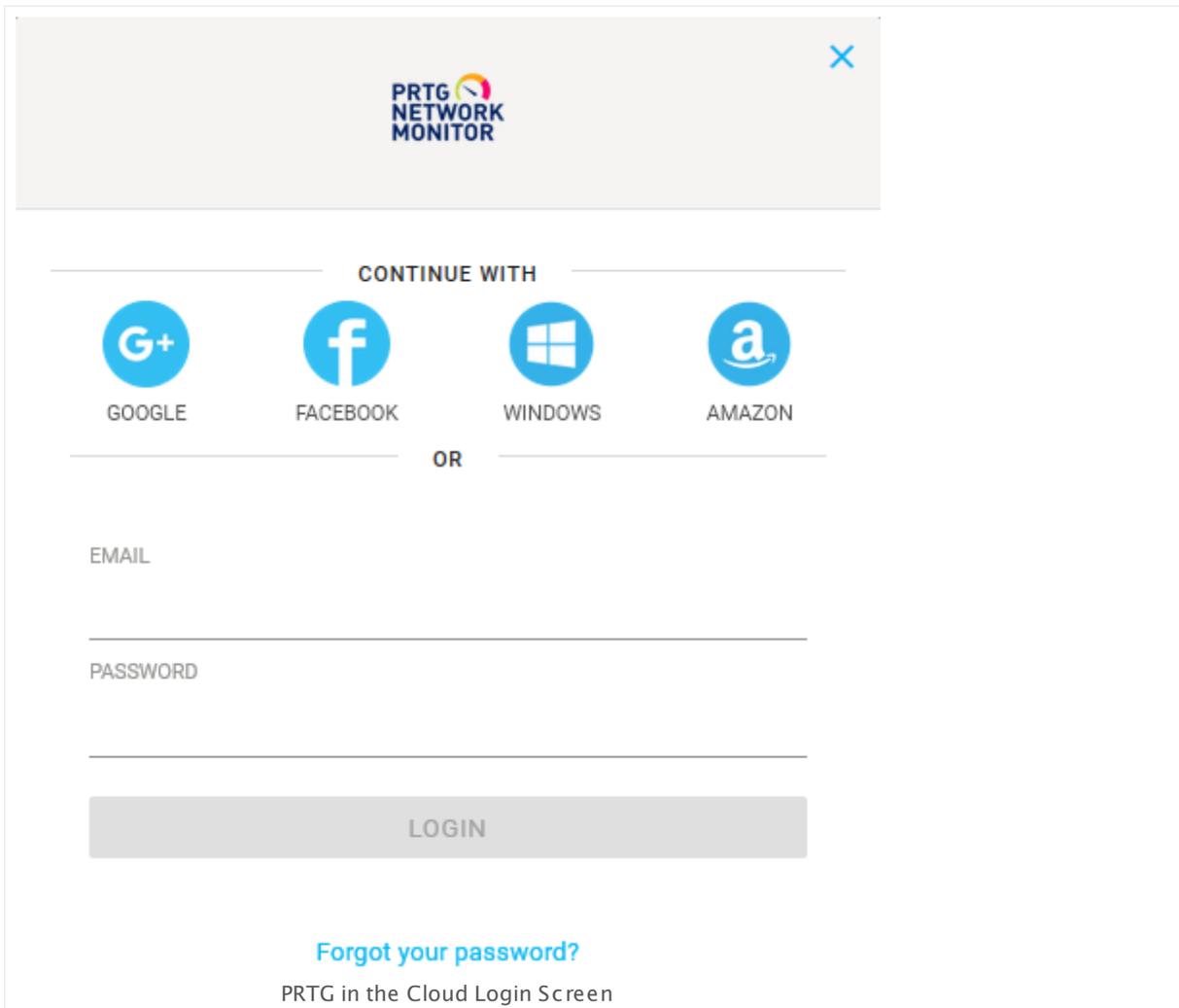
How Automatic Inventory Can Make Your Life Easier...
 Companies need a complete overview of their own IT infrastructure. The rapid pace of change requires the inventory overview to be frequently updated. Using Excel spreadsheets to maintain the inventory overview is limiting: inflexible, error-prone.

It's Time for Your SysAdmin Day Resolution: Invest i...
 SysAdmin Day is coming up on Friday, July 28th. This year, how about celebrating the day (and the coming year) with a resolution to invest in yourself to boost your skills and advance your career? Making a commitment to professional development

Why You Should Enable HTTPS on Your Website (Ye...
 There are Many Reasons in Favor of HTTPS and None (Really) Against It

PRTG Login Screen

- The default administrator credentials (login name **prtgadmin** and password **prtgadmin**) are automatically filled in. Select **Login** to proceed if you use PRTG on premises.



- If you use PRTG hosted by Paessler, click one of the social login buttons and log in with the according credentials using **Auth0**, or enter your dedicated my-prtg.com credentials and click **Login**. See section [Create a PRTG hosted by Paessler Instance](#)^[63] for more information on how to get started with PRTG hosted by Paessler.

Make sure you use a supported web browser when logging in to PRTG. Please use Google Chrome 67 or later (recommended), Mozilla Firefox 61 or later, or Microsoft Internet Explorer 11.

-  See the next step for more information about the initial configuration of PRTG using the [Smart Setup](#)^[52].

More

Video tutorials for PRTG Network Monitor:

- <https://www.paessler.com/support/videos>

2.2 TWO—Smart Setup

PRTG will automatically start the **Smart Setup** on a new PRTG instance. This setup assistant, represented by a member of the Paessler team, will guide you through the initial setup of your network monitoring system. The Smart Setup will reappear until you have completed all steps. You can skip the introduction altogether right at the beginning.

The Smart Setup in PRTG hosted by Paessler differs in some details from the Smart Setup in PRTG on premises. For example, it will ask you right at the beginning to [install a remote probe](#) in your local network. This is required to monitor your LAN, so we strongly recommend that you follow the smart setup!

First Start

When logging in for the first time, PRTG will show you the [device tree](#). PRTG on premises already contains several [devices](#) with [sensors](#) that monitor your network, ordered in different suitable [groups](#). PRTG automatically creates the device tree during the installation process by using its [Auto-Discovery](#) function. You do not have to fill out any forms but will directly see the availability and first monitoring results of various devices in your network when you first start PRTG!

PRTG scans your network by pinging IP addresses in the subnet of your PRTG system and adds all reachable devices to your specific network monitoring structure.

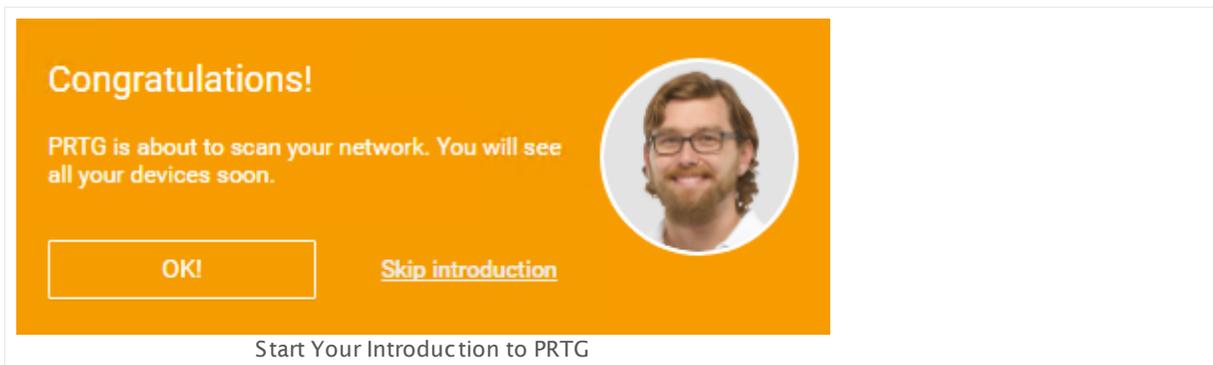
The smart setup scans only for devices with IP addresses in private network ranges. You can manually start an auto-discovery for other subnets later.

Device Tree after Initial Auto-Discovery

You will notice a Paessler employee in the upper-right corner of the PRTG web interface. He will guide you through 5 simple setup steps where you can enter more information about your network. PRTG will run another auto-discovery with this information to add additional devices and sensors to your monitoring. Of course, you can still edit the monitoring settings provided during the Smart Setup later on. And you can always adjust the monitoring to your needs.

Click **OK!** to start a guided tour, follow the instructions, and discover your network with PRTG!

i If you choose **Skip introduction** now, then the Smart Setup assistant will never appear again! We strongly recommend that you take the guided tour if you are new to PRTG.

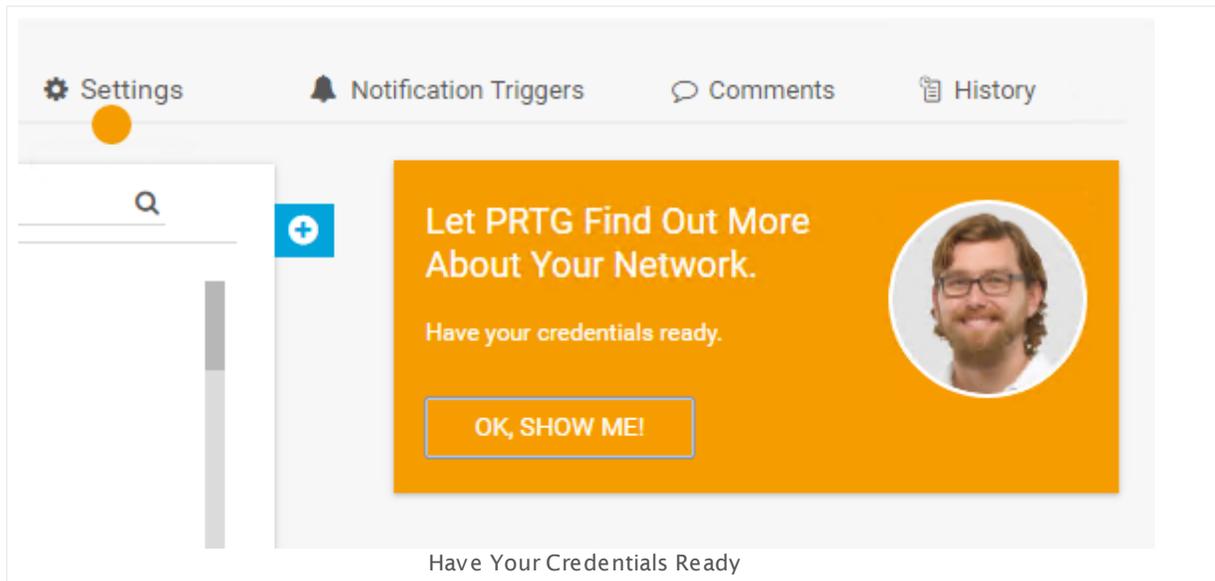


The steps to take are:

- [Provide Credentials](#)^[53]
- [Enter Location Information](#)^[56]
- [Change Your PRTG Login Password](#)^[56]
- [Confirm Your Email Address](#)^[57]
- [Switch to SSL](#)^[58] (if you access PRTG from another computer)

Step 1: Provide Credentials

Your personal setup assistant Greg asks you to provide credentials for devices in your network. Click **OK, show me!**, follow the animated yellow mouse pointer, and open the **Settings** tab of the **Root** group.



In the **Settings** tab, enter various administrator credentials for your network environment. With these credentials, PRTG can add a large number of additional devices and sensors automatically to your device tree. This way, PRTG helps you set up your network monitoring so there is no need for you to manually add every single device one by one.

Credentials for Windows Systems

Domain or Computer Name

User

Password

How Can PRTG Access Your Systems?

Please enter administrator credentials so PRTG can discover more sensors for your devices.



[OK, DONE!](#)

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems

User

Login Login via Password
 Login via Private Key

Password

For WBEM Use Protocol HTTP
 HTTPS

For WBEM Use Port Set automatically (port 5988 or 5989)
 Set manually

SSH Port

SSH Rights Elevation Run the command as the user connecting (default)
 Run the command as another user using 'sudo' (with password)
 Run the command as another user using 'sudo' (without password)
 Run the command as another user using 'su'

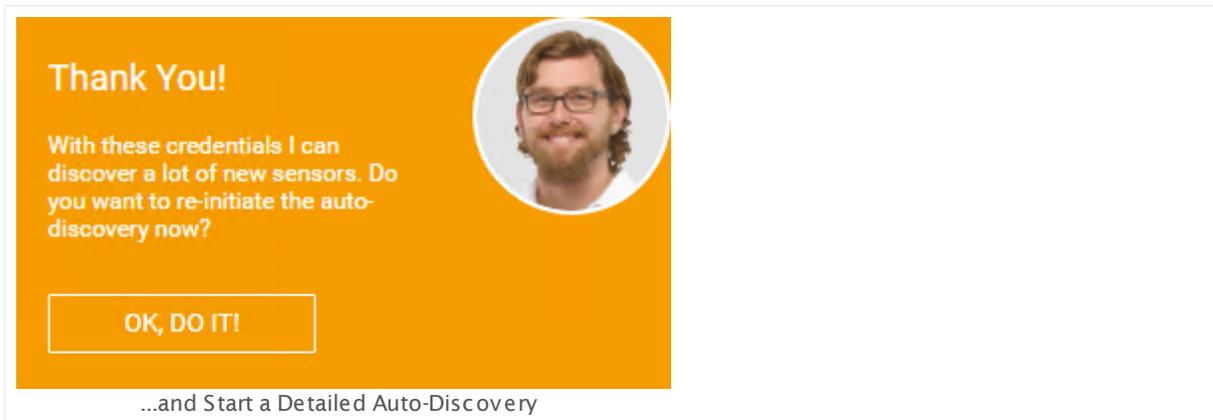
SSH Engine Default (recommended)
 Compatibility Mode (deprecated)

Provide Credentials...

- To monitor your Windows clients and servers via Windows Management Instrumentation (WMI), enter Windows administrator credentials for your network. We recommend that you use Domain Administrator credentials (if you use an Active Directory). For a general introduction to the technology behind WMI, see the manual section [Monitoring via WMI](#)^[3507].
- If you have systems running on Linux, Solaris, or Mac OS X, enter root access credentials for these systems. For a general introduction to SSH monitoring, see the manual section [Monitoring via SSH](#)^[3510].
- If you use the virtual environments VMware or Citrix XenServer, enter root access credentials for these systems. For a general introduction to the monitoring of virtual environments, see the manual section [Monitoring Virtual Environments](#)^[3527].
- To monitor your hardware (router, switches, etc.), Simple Network Management Protocol (SNMP) is the most commonly used protocol. Usually, all SNMP-enabled devices use the same settings by default: SNMP v2c, community string **public**, and SNMP port **161**. For a general introduction to the technology behind SNMP, see the manual section [Monitoring via SNMP](#)^[3489].

PRTG will store these credentials in the [Root](#)^[331] group of your device tree. All dependent devices automatically inherit and use them for monitoring. You can discontinue [Inheritance of Settings](#)^[137] at any level if you enter other credentials instead.

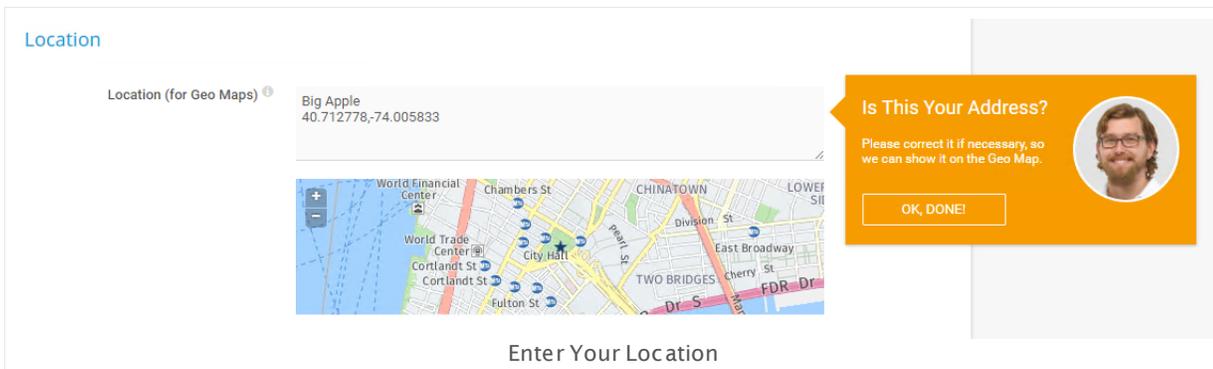
Click **OK, done!** to finish this setup step and confirm to start a detailed auto-discovery with the **OK, do it!** button.



For details about the available options, see the manual section [Root Group Settings](#)³³².

Step 2: Enter Location Information

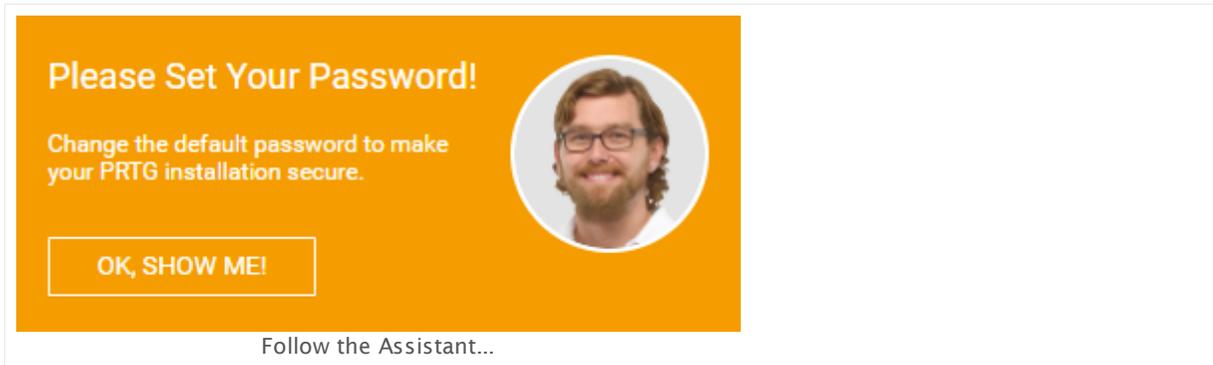
While PRTG runs a new auto-discovery in your network with the provided credentials, the setup assistant asks you to provide the location of your PRTG server. This information will be displayed on PRTG [Geo Maps](#)³²¹. Enter your location and confirm with **OK, done!**. Click **OK, show me!** to get back to the device tree.



For details about the available options, see the manual section [Root Group Settings](#)³³¹.

Step 3: Change Your PRTG Login Password

Back on the device tree, the PRTG on premises setup assistant asks you to change your password. Click **OK, show me!** and follow the assistant to your account settings. By default, PRTG uses the administrator account with login name **prtadmin** and password **prtadmin**. So we strongly recommend that you change the password to secure your PRTG installation against unauthorized access.



Please Set Your Password!

Change the default password to make your PRTG installation secure.

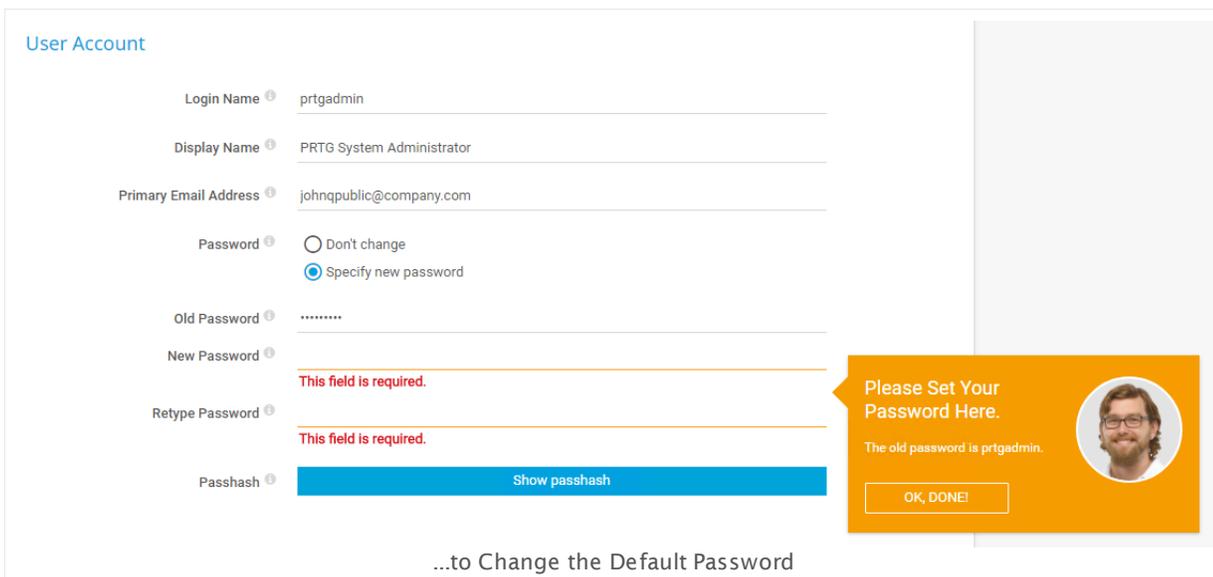
OK, SHOW ME!

Follow the Assistant...

Enter your **New Password**, confirm it with **Retype Password**. The password must meet the following requirements:

- at least eight characters long
- at least one numeral
- at least one capitalized letter

Click **OK, done!** to save your new password.



User Account

Login Name [ⓘ] prtgadmin

Display Name [ⓘ] PRTG System Administrator

Primary Email Address [ⓘ] johnqpublic@company.com

Password [ⓘ] Don't change
 Specify new password

Old Password [ⓘ]

New Password [ⓘ]
This field is required.

Retype Password [ⓘ]
This field is required.

Passhash [ⓘ]

...to Change the Default Password

Please Set Your Password Here.

The old password is prtgadmin.

OK, DONE!

 For details about the available options, see the manual section [Account Settings—My Account](#) ³³⁰⁴.

Step 4: Confirm Your Email Address

To complete the PRTG Smart Setup, check whether the email address that you have entered during the installation is correct.

 A working email address is absolutely mandatory for PRTG to reach you via email notifications, alarms, and for other important messages.

If the address is correct, click **OK, done!** and follow the assistant back to the device tree.

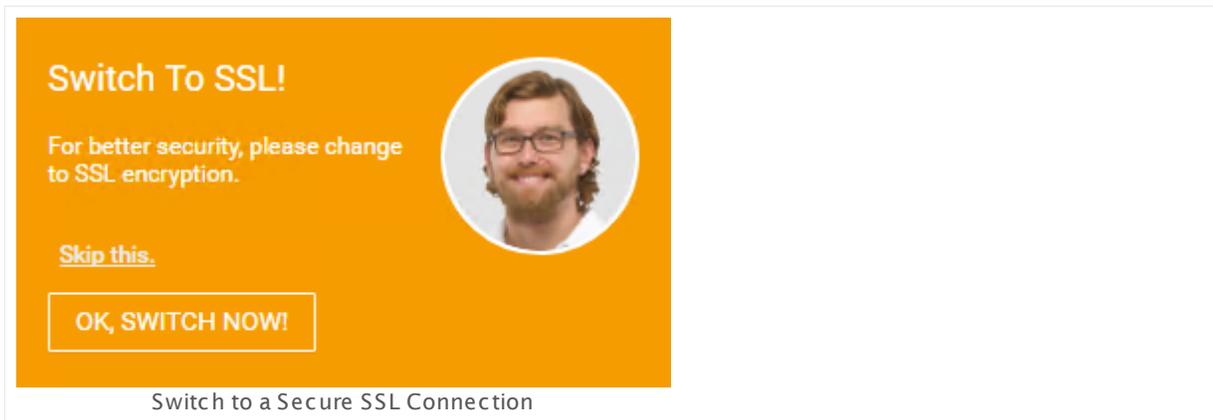
The screenshot shows the 'Account Settings' interface. At the top, there are tabs for 'My Account', 'Notification Templates', 'Notification Contacts', and 'Schedules'. The 'My Account' tab is active. Below the tabs, there are sections for 'Mobile App' and 'User Account'. The 'Mobile App' section has a 'Use Mobile App' button and a 'Show QR code for Mobile App Login' button. The 'User Account' section contains input fields for 'Login Name' (prtgadmin), 'Display Name' (PRTG System Administrator), and 'Primary Email Address' (johnpublic@company.com). There are radio buttons for 'Password' (Don't change) and 'Specify new password', and a 'Show passhash' button. An orange notification box on the right side of the form says 'Please Verify Your Email Address. This way PRTG informs you about alarms and other notifications.' and has an 'OK, DONE!' button. At the bottom of the form, it says 'Verify Your Email Address'.

For details about the available options, see the manual section [Account Settings—My Account](#)³³⁰⁴.

Step 5: Switch to SSL

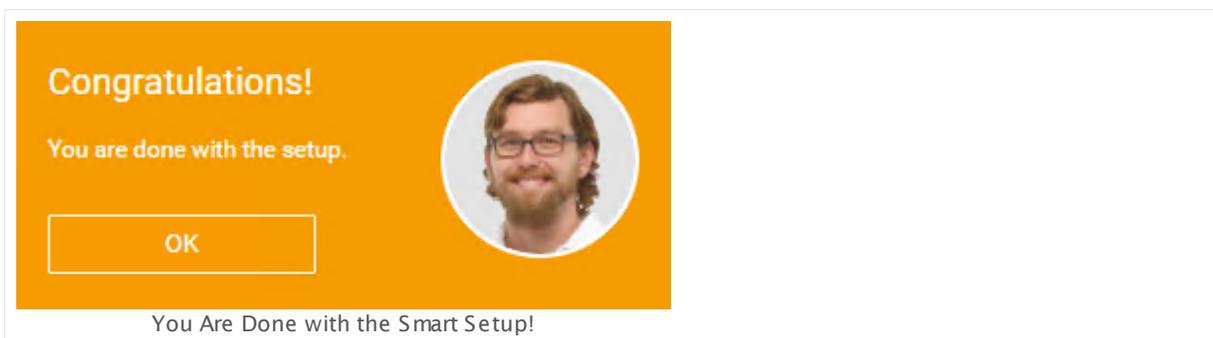
If you access the PRTG on premises web interface from a computer other than the computer where you installed PRTG, the assistant will appear and ask you to switch to a secure connection with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption. We strongly recommend that you run the PRTG web interface using SSL encryption (Hypertext Transfer Protocol Secure (HTTPS)), especially if you make your web interface available from the internet. Without encryption, your passwords are sent unencrypted over your network.

- Click **OK, switch now!** to get more information about using SSL for the PRTG web server.
- In the new window, click the button **Yes, switch to SSL now** to switch to an SSL-encrypted connection.
- PRTG must restart its services to apply the changes and is reachable under an **HTTPS** URL afterwards.
- When the web interface reloads, most likely it will show a [certificate warning](#)¹⁷². Confirm it to proceed to the login screen.



For more details, see the manual sections [System Administration—User Interface](#)^[3346] and [SSL Certificate Warning](#)^[172].

You Are Done!



While you were busy with the Smart Setup, PRTG created additional devices and sensors for you. There are first monitoring values available, too. Now you are all-in in your personal unified network monitoring!

 To become familiar with the PRTG web interface, we recommend that you read on in the manual section [General Layout](#)^[187] of the web interface.

More

Video Tutorial: PRTG Installation and Smart Setup

- https://www.paessler.com/support/videos/prtg-basics/installation_of_prtg_network_monitor

Part 3

Using PRTG Hosted by Paessler

3 Using PRTG Hosted by Paessler

PRTG Network Monitor offers two options to monitor your network: PRTG on premises and PRTG hosted by Paessler. With PRTG on premises, the core server and local probe run within your network. PRTG hosted by Paessler is the PRTG cloud solution, where we at Paessler run the core server and hosted probe for you. The [PRTG web interface](#)^[168] for monitoring configuration and reviewing monitoring data is the same for both, PRTG hosted by Paessler and PRTG on premises.

The following sections show you how to [Create a PRTG hosted by Paessler Instance](#)^[63] and how to [Manage a PRTG hosted by Paessler Subscription](#)^[71].



See the Paessler website for [PRTG hosted by Paessler – Service Description](#) and [FAQ – PRTG hosted by Paessler](#).

More

Paessler Website: PRTG hosted by Paessler – Service Description

- <https://www.paessler.com/prtg/prtg-in-the-cloud-service-description>

Paessler Website: FAQ – PRTG hosted by Paessler

- <https://www.paessler.com/support/faqs/faq-prtg-in-the-cloud>

PRTG Manual:

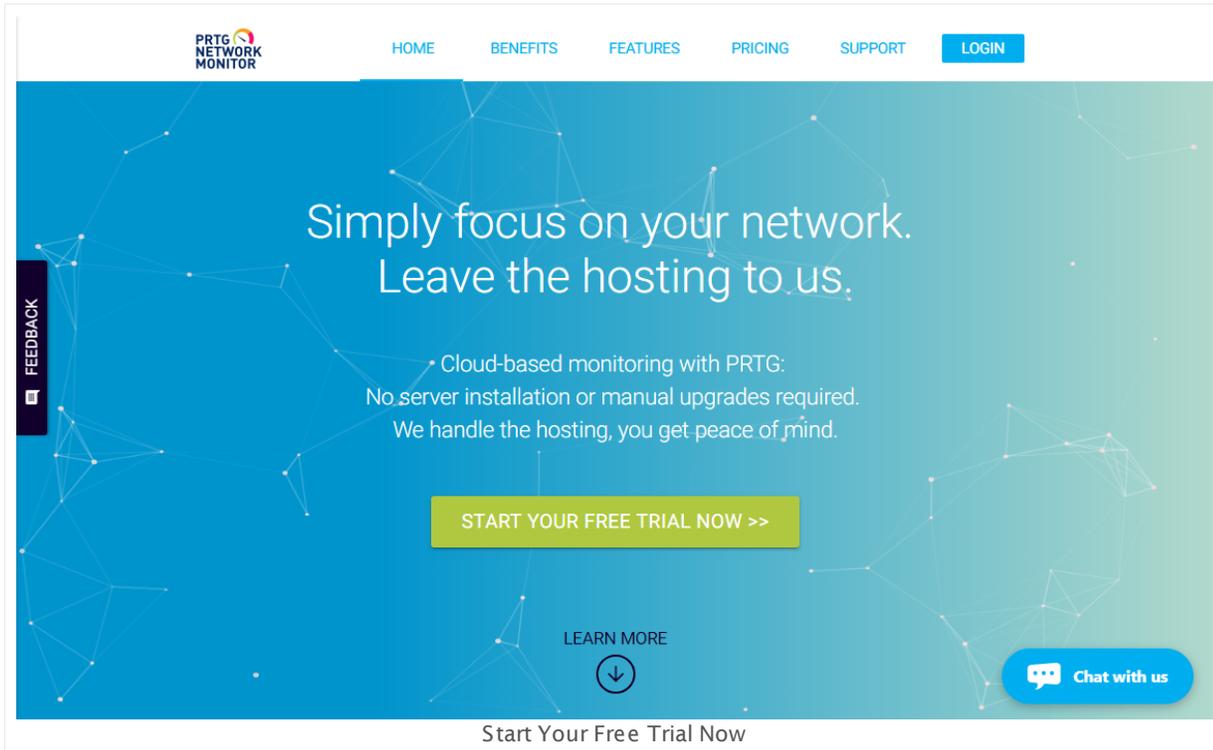
- [Differences between PRTG on Premises and PRTG hosted by Paessler](#)^[3756]

Using PRTG hosted by Paessler—Topics

- [Create a PRTG hosted by Paessler Instance](#)^[63]
- [Manage a PRTG hosted by Paessler Subscription](#)^[71]

3.1 Create a PRTG Hosted by Paessler Instance

To create a PRTG hosted by Paessler instance, open your web browser (Google Chrome 67 or later (recommended)) and go to <https://my-prtg.com>. This is the PRTG hosted by Paessler web portal.



The screenshot shows the PRTG Network Monitor website. The header includes the PRTG Network Monitor logo and navigation links: HOME, BENEFITS, FEATURES, PRICING, SUPPORT, and LOGIN. The main content area features a blue background with a network diagram. The headline reads: "Simply focus on your network. Leave the hosting to us." Below this, a bullet point states: "Cloud-based monitoring with PRTG: No server installation or manual upgrades required. We handle the hosting, you get peace of mind." A prominent yellow button says "START YOUR FREE TRIAL NOW >>". Below the button is a "LEARN MORE" link with a downward arrow icon. In the bottom right corner, there is a "Chat with us" button. A vertical "FEEDBACK" button is visible on the left side. At the bottom of the page, the text "Start Your Free Trial Now" is displayed.

Click **Start Your Free Trial Now** to create your PRTG hosted by Paessler instance. PRTG hosted by Paessler automatically assigns a domain name to your instance. You can change this in the [Dashboard](#)^[73] at any time.

PAESSLER
THE NETWORK MONITORING COMPANY

Sign Up

Log In Sign Up

G f a Windows

or

yours@example.com

your password

By signing up I agree to the [terms and conditions](#) and [privacy policy](#).

SIGN UP >

Sign Up to PRTG Hosted by Paessler

You can sign up with your Google+, Facebook, Windows, or Amazon account via single sign-on (Auth0). This account will then always be automatically used for login and will be connected to your PRTG hosted by Paessler account. Just click the respective button and follow the instructions there.

Alternatively, you can sign up via email by entering a valid **Email** address, a **Password**, and confirming it with **Confirm Password**. The password must meet the following requirements:

- at least 8 characters long
- at least one uppercase letter
- at least one lowercase letter
- at least one numeral

Make sure to agree to the terms and conditions and privacy policy. Click **Sign Up** to register for your PRTG hosted by Paessler instance. PRTG then notifies you that a verification email has been sent to your inbox.



Thank you for signing up. Please check your email inbox, we have just sent you an email to verify your email address.

Go to your inbox and open the email.



VERIFY EMAIL ADDRESS

Thank you for signing up for PRTG.

We need you to [click below](#) before we get started.

VERIFY EMAIL ADDRESS >>

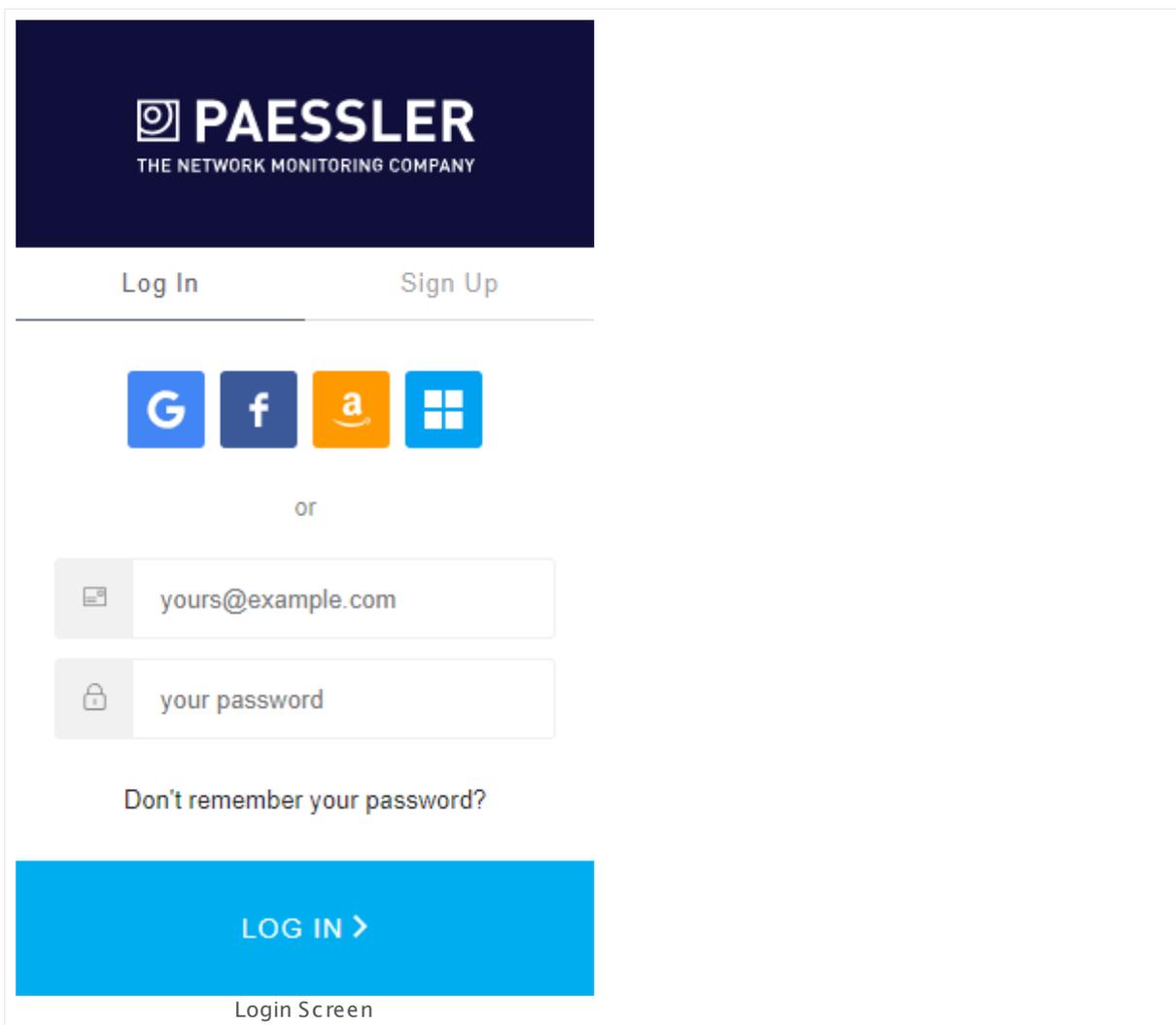
If you have any issues with your account, please don't hesitate to contact us at support@paessler.com.



Enjoy monitoring,
YOUR PRTG

Verify Email Address

Click **Verify Email Address** to verify your email address and go to the login screen.



PAESSLER
THE NETWORK MONITORING COMPANY

Log In Sign Up

G f a Microsoft

or

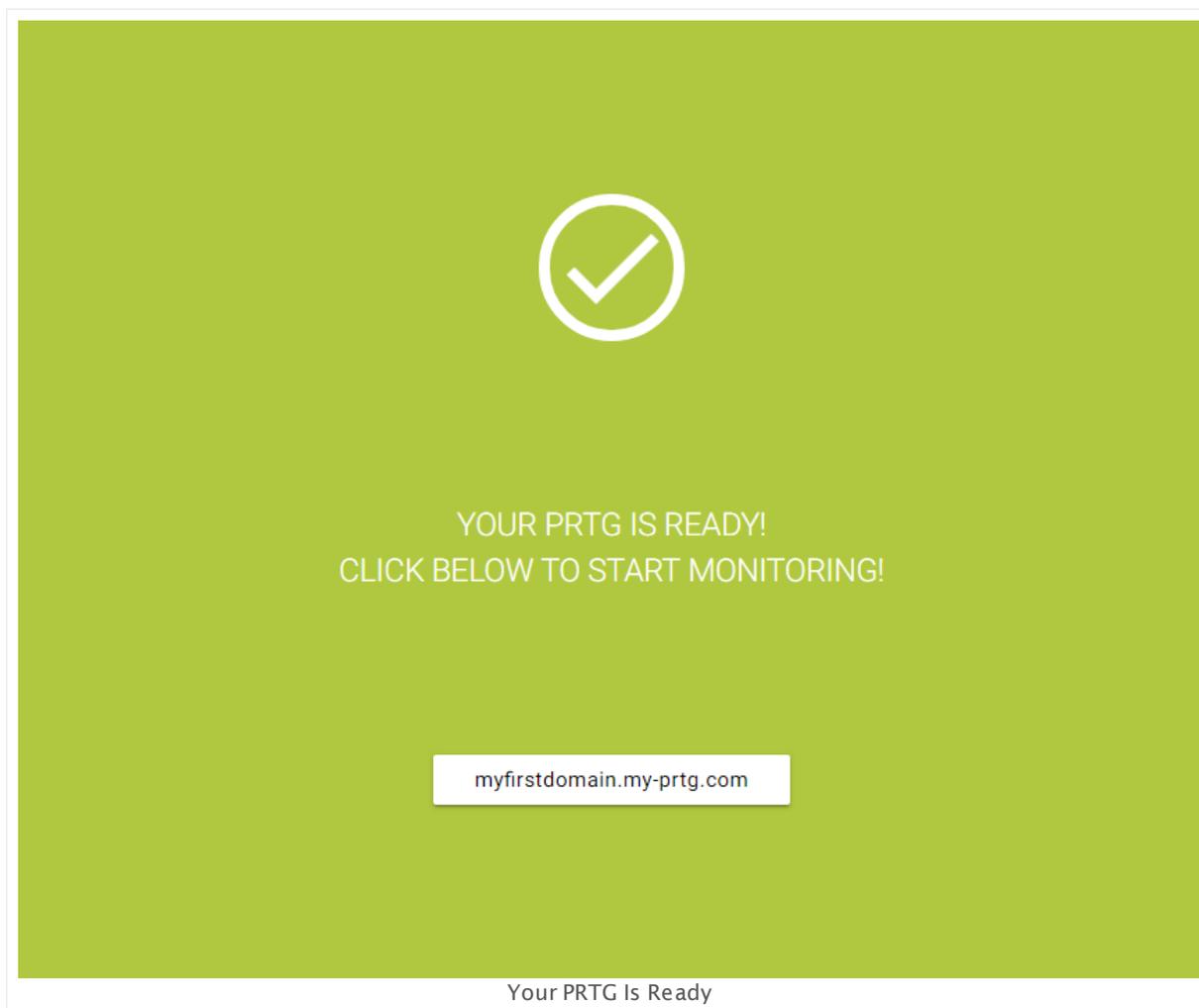
Don't remember your password?

LOG IN >

Login Screen

Enter your credentials and click **Login** to log in to PRTG hosted by Paessler.

While we prepare your subscription, a welcome video plays that introduces the basics of network monitoring with PRTG hosted by Paessler.



When your subscription is ready, click the URL with your domain to open the [PRTG web interface](#)¹⁶⁶.

Part 3: Using PRTG Hosted by Paessler | 1 Create a PRTG Hosted by Paessler Instance

The screenshot displays the PRTG Network Monitor interface. At the top, there's a navigation bar with options like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A search bar and 'New Log Entries 3' are also visible. The main header area says 'Welcome John Q. Public!' and includes a 'TRUSTPILOT' rating section. Below this, two large circular gauges show 'All Sensors' with a value of 4 and 'Current Alarms' with a value of 0. To the right of the 'All Sensors' gauge is a legend for sensor states: Down (0), Down (Acknowledged) (0), Warning (0), Up (4), Paused (0), Unusual (0), and Unknown (0). Below the gauges are three main content blocks: 'Your PRTG' with links for 'View Results', 'Install Smartphone App', 'Get Help and Support', and 'Manage Subscription'; 'Yesterday's Activity' showing 0 for Sensor Scans Performed, Sensor State Changes, Notifications Sent, Reports Generated, and Web Pages Served; and 'Paessler Blog' with several article titles like 'Monitoring Healthcare IT With PRTG: A Video' and 'Monitor Your Palo Alto Firewall with PRTG'. At the bottom, there's a 'Welcome' message and a 'View All Tickets' button showing 1 ticket.

Congratulations, your PRTG hosted by Paessler instance is up and running! To open the device tree, click **View Results** or **Devices** in the [main menu bar](#)^[263].

PRTG hosted by Paessler has automatically created a **Hosted Probe** that runs on the hosted PRTG instance. It shows several health values of the instance and you can instantly monitor all servers, services, and devices that are publicly available via the internet with this probe. See also section [Architecture and User Interfaces—Probe\(s\)](#)^[126].

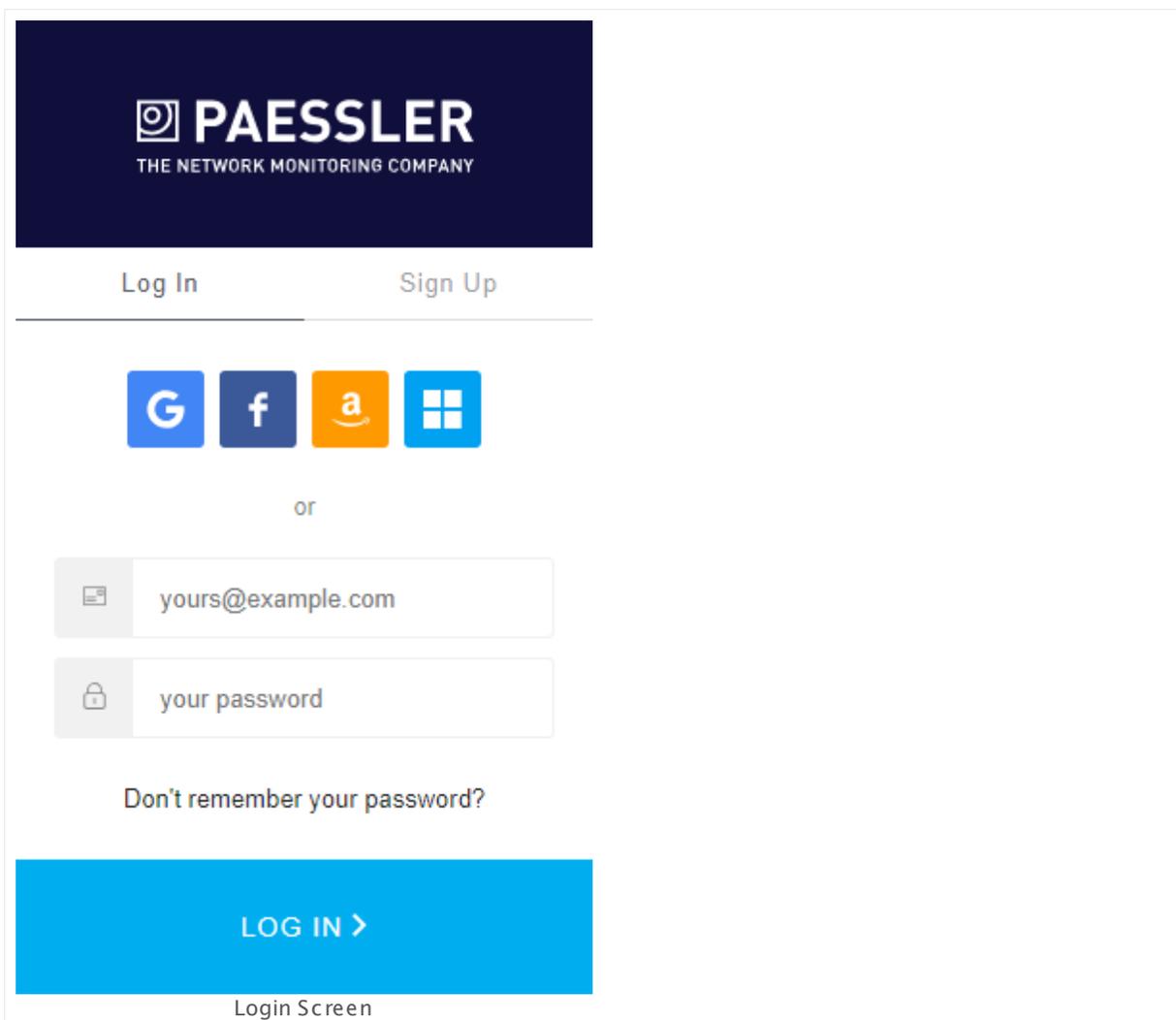
A Paessler employee will guide you through the [Smart Setup](#)^[52]. In particular, you will install a [remote probe](#)^[370], which is required for monitoring your LAN. We strongly recommend that you follow the instructions for best monitoring experience!

3.2 Manage a PRTG Hosted by Paessler Subscription

PRTG Network Monitor offers **Monitoring as a Service** with PRTG hosted by Paessler. PRTG hosted by Paessler runs in the cloud and does not require a PRTG core server installation inside your network, making monitoring even easier. We offer subscription plans that you can tailor to your needs and manage via the PRTG hosted by Paessler web portal on my-prtg.com.

All you need to do is open a web browser (Google Chrome 67 or later (recommended)), go to <https://my-prtg.com>, and log in to manage your subscription.

 For details about setting up a PRTG hosted by Paessler instance, see manual section [Create a PRTG Hosted by Paessler Instance](#)⁶³¹.



PAESSLER
THE NETWORK MONITORING COMPANY

Log In Sign Up

G f a Windows

or

yours@example.com

your password

Don't remember your password?

LOG IN >

Login Screen

Provide the credentials you entered when signing up and click **Login** or use single sign-on and continue with your Google+, Facebook, Windows, or Amazon account via the respective button.

System Status

The **System Status** gives you an overview of the overall status of PRTG hosted by Paessler, including services and features. Clicking the icon opens a new browser window.

The screenshot shows the PRTG System Status page. At the top left is the PRTG Network Monitor logo. Below it, the text reads "System status for PRTG hosted by Paessler" next to a "SUBSCRIBE TO UPDATES" button. A green bar below this indicates "All Systems Operational". The "About This Site" section explains that this is the status page for PRTG hosted by Paessler. Below this is a table with the following data:

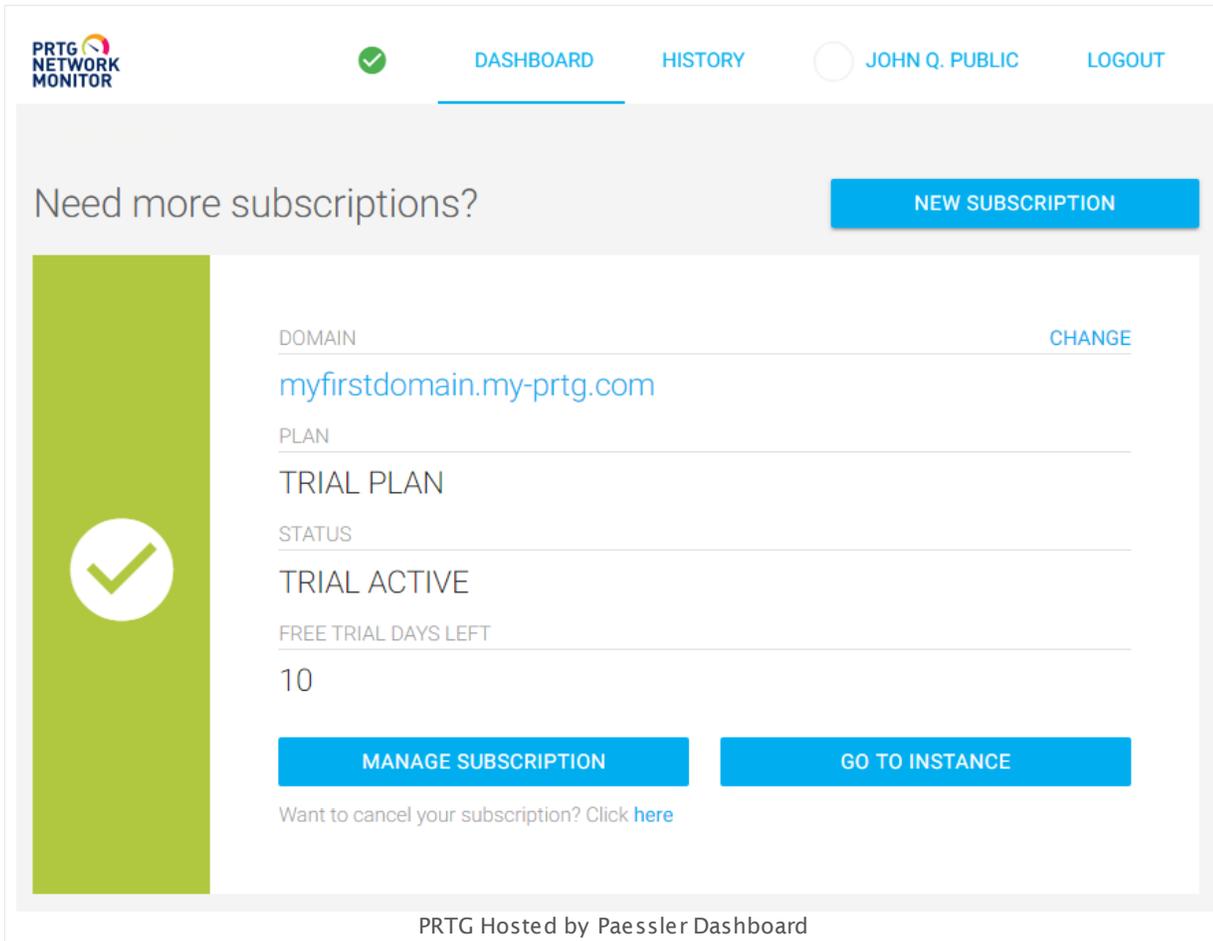
⊞ PRTG Instances	Operational
⊞ my-prtg.com	Operational
Authentication	Operational
⊞ Subscriptions	Operational

System Status

Here you can see the status of your PRTG instances, my-prtg.com, authentication, and your subscriptions. You can also see a list of reported incidents such as version updates or scheduled maintenance. If you want to receive updates when there are issues, click the **Subscribe to Updates** button. You can receive updates via email or SMS text message. You can also contact support or view web feeds.

Dashboard

The **Dashboard** tab gives you an overview of your PRTG hosted by Paessler subscription. Here you can manage or cancel your subscription, or add a new subscription. If you have purchased a subscription, you will also see when your next payment is due. You can also click the link under **Domain** to open the [PRTG web interface](#) or click **Change** to change the domain name. The domain name can be anywhere from 4 and 60 characters long. Enter a domain name of your choice, such as **myfirstdomain**. So if you enter **myfirstdomain** as the domain name here, your PRTG hosted by Paessler instance will be reachable under **myfirstdomain.my-prtg.com**.



The screenshot shows the PRTG Network Monitor dashboard. At the top left is the PRTG Network Monitor logo. To its right is a green checkmark icon. Further right are navigation links: **DASHBOARD** (underlined), **HISTORY**, **JOHN Q. PUBLIC** (with a profile icon), and **LOGOUT**. Below the navigation is a header area with the text "Need more subscriptions?" and a blue button labeled "NEW SUBSCRIPTION". The main content area features a green vertical bar on the left with a white checkmark icon. To the right of this bar, the subscription details are displayed in a list format:

- DOMAIN**: myfirstdomain.my-prtg.com (with a "CHANGE" link to the right)
- PLAN**: TRIAL PLAN
- STATUS**: TRIAL ACTIVE
- FREE TRIAL DAYS LEFT**: 10

At the bottom of this section are two blue buttons: "MANAGE SUBSCRIPTION" and "GO TO INSTANCE". Below these buttons is a link: "Want to cancel your subscription? Click here". At the very bottom of the dashboard area, the text "PRTG Hosted by Paessler Dashboard" is centered.

Click **Manage Subscription** to view your subscription details. The following information is displayed where you can edit your plan, payment, or billing address. Click **Change Plan** to save your changes.

MANAGE SUBSCRIPTION

① PLAN

Plan Name	Price	Frequency	Sensors
PRTG 500	\$149	per month	500 SENSORS
PRTG 1000	\$249	per month	1000 SENSORS
PRTG 2500	\$549	per month	2500 SENSORS
PRTG 5000	\$899	per month	5000 SENSORS

③ PAYMENT

④ BILLING

⑤ SUMMARY

Manage Subscription

Click **New Subscription** to add a new subscription to your account.

New Subscription

- PLAN** DONE

TRIAL PLAN
FREE for 10 days
500 SENSORS

Trial limit exceeded

PRTG 500 \$ 149 per month 500 SENSORS	PRTG 1000 \$ 249 per month 1000 SENSORS	PRTG 2500 \$ 549 per month 2500 SENSORS	PRTG 5000 \$ 899 per month 5000 SENSORS
--	--	--	--
- DOMAIN**

Name: Domain name will be generated unless you click "CHANGE" to provide your own.
- PAYMENT**

Credit Card Number * Expiry Date * CVC *

Please fill out all required (*) fields
- BILLING**
- SUMMARY**

By starting a new subscription

Add a New Subscription

Enter a domain name, for example [myseconddomain.my-prtg.com](#), choose a plan, and then enter your credit card information and billing address. Click **Subscribe Now** to add the subscription.

Click the **Cancel Subscription** link to cancel your PRTG hosted by Paessler subscription. Enter **CANCEL** in the field and click the **Cancel Subscription** button to finalize the cancellation.

CANCEL SUBSCRIPTION

ARE YOU SURE YOU WANT TO CANCEL THIS SUBSCRIPTION?

Type in **CANCEL** to confirm

CANCEL SUBSCRIPTION CLOSE

Cancel a Subscription

History

This tab gives you an overview of the history of your subscriptions.

PRTG NETWORK MONITOR ✓ DASHBOARD HISTORY ○ JOHN Q. PUBLIC LOGOUT

NOW

Subscription Created
Subscription was created. ✓ JUL 27, 2018

JUL 27, 2018 ✗ Subscription Cancelled
Subscription was cancelled.

Subscription Created
Subscription was created. ✓ JUL 27, 2018

Account Created
A user account **John Q. Public** was created. NEW JUL 27, 2018

Subscription History

Account Settings—Profile

Here you can view your profile, view or update your payment information, and view your invoices.

Account Settings—Payment

When purchasing a subscription, you will need your payment information. Enter your credit card information and billing address here to save it for later use.

PRTG NETWORK MONITOR ✓ [DASHBOARD](#) [HISTORY](#) [JOHN Q. PUBLIC](#) [LOGOUT](#)

[PROFILE](#) [PAYMENT](#) [INVOICES](#)

! Missing payment / billing information

Payment details

Credit Card Number * Expiry Date * CVC *

Please fill out all required (*) fields

Billing details

Company Name VAT ID
DE 217564187

First Name * Last Name *

Country *

Street Address * Zip Code * City *

Please fill out all required (*) fields

Payment Information

Account Settings—Invoices

Here you can view and download all of your invoices.

Logout

Click **Logout** in the upper-right corner to log out of your account.

Part 4

Installing the Software

4 Installing the Software

The following sections show you how to download and install your PRTG on premises instance. If you want to use PRTG hosted by Paessler, just go straight to section [Create a PRTG hosted by Paessler Instance](#)^[63] to get started.

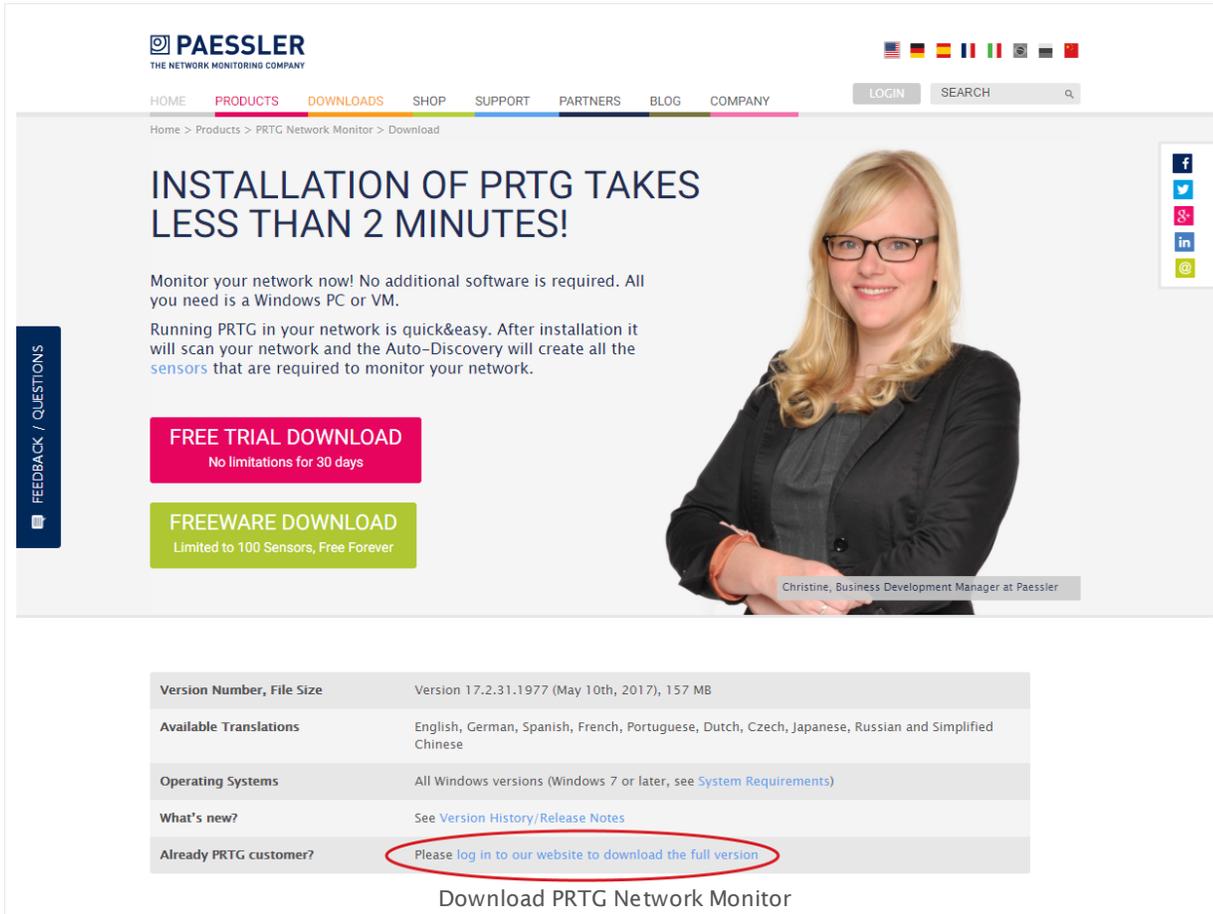
Installing the Software—Topics

- [Download PRTG](#)^[81]
- [Update From Previous Versions](#)^[83]
- [Install a PRTG Core Server](#)^[89]
- [Create a PRTG hosted by Paessler Instance](#)^[63]
- [Install a PRTG Cluster](#)^[95]
- [Enter a License Key](#)^[96]
- [Activate the Product](#)^[99]
- [Install a PRTG Remote Probe](#)^[101]
- [Install the Enterprise Console](#)^[113]
- [Uninstall PRTG Products](#)^[119]

4.1 Download PRTG

You can find the installer for PRTG on our website <https://www.paessler.com>. There you can also login to the Paessler shop to buy or upgrade your license, or to renew your maintenance.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.



PAESSLER
THE NETWORK MONITORING COMPANY

HOME PRODUCTS DOWNLOADS SHOP SUPPORT PARTNERS BLOG COMPANY LOGIN SEARCH

Home > Products > PRTG Network Monitor > Download

INSTALLATION OF PRTG TAKES LESS THAN 2 MINUTES!

Monitor your network now! No additional software is required. All you need is a Windows PC or VM.

Running PRTG in your network is quick&easy. After installation it will scan your network and the Auto-Discovery will create all the **sensors** that are required to monitor your network.

FREE TRIAL DOWNLOAD
No limitations for 30 days

FREEMWARE DOWNLOAD
Limited to 100 Sensors, Free Forever

Christine, Business Development Manager at Paessler

Version Number, File Size	Version 17.2.31.1977 (May 10th, 2017), 157 MB
Available Translations	English, German, Spanish, French, Portuguese, Dutch, Czech, Japanese, Russian and Simplified Chinese
Operating Systems	All Windows versions (Windows 7 or later, see System Requirements)
What's new?	See Version History/Release Notes
Already PRTG customer?	Please log in to our website to download the full version

Download PRTG Network Monitor

Downloading PRTG Network Monitor

Please download the latest publicly available program version from the Paessler website. Simultaneously, you will receive a trial key. Enter this license key during the installation of PRTG. If you have already purchased a commercial license, use your commercial key. Please log in to the Paessler website to find your license key,

- <https://www.paessler.com/prtg/download>
- <https://shop.paessler.com/accounts/login/>

Every freeware installation starts as a trial version that allows you to use an unlimited number of sensors for 30 days. After the trial period has expired, your installation automatically reverts to the freeware edition with 100 sensors. Please understand that customers with a commercial license get prioritized support.

To upgrade your running trial or freeware version to a commercial edition, please purchase a commercial license key on <https://shop.paessler.com> and enter this key on the [license page](#)  in the PRTG web interface.

Updates are free to customers with an active maintenance contract. If you do not have an active maintenance contract, please log in to the Paessler shop to renew it or contact sales@paessler.com.

 Once installed, the PRTG [Software Auto-Update](#)  will automatically download and install new software versions. This helps you keep PRTG up to date without manually installing new PRTG versions.

4.2 Update From Previous Versions

If you already have a previous software version installed, there are several things you have to consider before you update to the current PRTG version. Please see section [Detailed System Requirements](#)^[26] to see all requirements for the current PRTG version.

 We recommend that you always have a proper backup of your monitoring data and configuration. In most cases both will be maintained when upgrading. Anyway, we recommend a backup before upgrading. For details, see the Knowledge Base: [How do I backup all data and configuration of my PRTG installation?](#)

 In certain cases, antivirus software like Windows Defender interfere with the PRTG installer. This might cause high CPU load on the PRTG server, which might prevent a successful update of PRTG. Please temporarily disable Windows Defender and other antivirus software if you have issues installing PRTG updates.

 On PRTG hosted by Paessler instances, the update process is managed automatically, so you do not have to care about updating your PRTG.

Update from PRTG Network Monitor 16.1.22 or later

If you run PRTG Network Monitor with version 16.1.22 or later, simply [install](#)^[89] the latest version on top of the previous version. Your configuration will be kept. PRTG updates [remote probes](#)^[379] automatically as well. If you have configured PRTG as a [cluster](#)^[130], you only have to install an update on any node server (master or failover). PRTG deploys the new version to the cluster automatically.

We recommend that you use the [Auto-Update](#)^[340] of PRTG to install the latest version. Please always have a proper backup of your monitoring data.

Important notes:

- **PRTG 17.3.34** comes with a completely rewritten web interface. If you have customized the PRTG web interface using one of the dedicated files in a prior version, all your customizations will be lost as soon as you install PRTG 17.3.34. You will have to redo your changes to keep the customizations. For details, see the Knowledge Base: [Customizing and Re-Branding the PRTG Web Interface](#)
- As of **PRTG 17.3.34**, sensor types that require the .NET framework need version .NET 4.5 or later. For details, see the Knowledge Base: [Which .NET version does PRTG require?](#)
- With **PRTG 16.3.26**, the Mobile Web GUI has been removed from PRTG.
- With **PRTG 16.2.25**, several sensor types have been [removed from PRTG](#)^[84].

Update from PRTG Network Monitor 13.1.1 through 16.1.21

As of version 16.1.22, PRTG is signed with renewed certificates. To be able to seamlessly update to version 16.1.22 or later an **intermediate update** is required for the PRTG core server and all probes if you currently run a PRTG version previous to 16.1.21.1691/1692. If you [auto-update](#)³⁴⁰⁷ from previous versions (lower than 16.1.21.1691/1692), PRTG will automatically install this intermediate version first. You have to perform an additional auto-update to install the latest version. PRTG will notify you with a [ticket](#)²³⁶¹ about this approach. Your configuration will be kept.

 We recommend that you use the [auto-update](#)³⁴⁰⁷ to install the latest PRTG version. If you update manually with an installer downloaded from the Paessler online shop, the intermediate update is only necessary if you currently run a PRTG version **previous to 16.1.21.1691/1692 with one or more remote probes or in a cluster setup**. If you do not perform this intermediate update, you will have to update your remote probes and cluster nodes manually. Please [contact our technical support team](#)³⁴²⁴ to get the installer for this version if you do not use the auto-update.

- As of PRTG 14, **Internet Explorer 9 is no longer officially supported** for access to the PRTG web interface.
- Also as of PRTG 14, PRTG core and probes no longer officially support **Windows XP and Windows Server 2003** (including SP1 and SP2).
- As of PRTG 15, **Internet Explorer 10 is no longer officially supported** for access to the PRTG web interface.

Removed Sensor Types as of PRTG Network Monitor 16.2.25

We have removed several sensor types from PRTG with version 16.2.25. Sensors of these types that you still use in your PRTG installation will stop monitoring and show a down status as soon as you update to 16.2.25 or later. Most of the affected sensor types have been deprecated as of PRTG version 16.2.23 or before. You will receive tickets from PRTG that inform you if your PRTG setup is affected.

These sensor types were used by very few PRTG users and/or created substantial load for both our technical support and development team. We believe that the majority of PRTG users prefers that we focus on features that many customers use everyday rather than spending our precious energy on niche issues. We want to keep PRTG as easy to use as possible!

 For a list of all discontinued sensors, possible alternatives, and more details about this approach, see this article: <https://kb.paessler.com/en/topic/68227>

Web Interface Customizations as of PRTG Network Monitor 13.2.3

As of PRTG version 13.2.3, the **website** folder of the PRTG program directory is not used anymore. This means that if you update from a PRTG version older than 13.2.3 to the current version, all existing customizations of the web interface will be disabled and you have to revise them. You may find a way for a similar customization that you can add to the files in the current **webroot** folder that contains the web interface files now.

 For details, see the Knowledge Base: [What about my web interface customizations as of PRTG 13.2.3?](#)

Update from PRTG Network Monitor 9 and 12

 We strongly recommend that you perform a clean install of the latest PRTG version instead of updating from an existing PRTG 9 or 12!

If you use PRTG 9 or 12 now, your configuration will be kept when installing the current PRTG version in **Standalone Mode** or when installing a **Master Node**. There are only a few things you should consider.

 We recommend that you always have a proper backup of your monitoring data.

- **Intermediate versions:** You have to install two intermediate versions before you can update to the latest version.
 - If you currently run PRTG version 12.4.5.3164/3165 or lower, install the **intermediate version 12.4.7.3507** before you proceed.
 - If you have installed version 12.4.7.3507, install the **intermediate version 16.1.21.1691/1692** before you proceed. Afterwards you can seamlessly update to the latest PRTG version. For details about this intermediate update, see section [Update from PRTG Network Monitor 13.1.1 through 16.1.21](#)^[84] above.
 - We recommend that you use the [Auto-Update](#)^[3407] feature. In this case PRTG will automatically install the intermediate versions. Run the auto-update three times if you come from a version previous to 12.4.7.3507, run it twice if you come from a version previous to 16.1.21.1691/1692. If you do not use the auto-update, please [contact our technical support team](#)^[3424] to get the installers for these intermediate versions.
- **Discontinued Sensors:** Existing instances of the following sensor types will stop working as of PRTG V12 and must be replaced with their successor sensor types!
 - VMware Host Server (SOAP)
 - VMware Virtual Machine (SOAP)
 - Xen Virtual Machine

If your configuration contains these sensor types, they will stop monitoring after upgrading to the current version. We recommend that you to pause them to keep their data. To continue monitoring, please add the sensors anew (for example, using the auto-discovery).

- **Please install .NET 4.0:** We strongly recommend that you install .NET 4.0 on systems that run the core server (and the remote probes, if you use those). Otherwise the following features will not work: [VMware](#)^[435] auto-discovery and monitoring, [Citrix XenServer](#)^[599] auto-discovery and monitoring, [SIP Options Ping Sensor](#)^[1786], Windows Last Update Sensor (deprecated as of PRTG 16.x.23).
- **Changed Geo Maps Provider:** When you update to the current PRTG version, the provider for geographical maps will automatically be switched from Google Maps to MapQuest (using Open Street Map data).

- **Windows 2000 Not Supported:** Since PRTG 7 we do not officially support Windows 2000 systems anymore. This means that PRTG cannot be installed on systems running Windows 2000, and you cannot officially monitor Windows 2000 systems (for example, via WMI). However, if you could successfully monitor your Windows 2000 systems with PRTG 9, this might actually not be possible anymore with the current PRTG version.
- ❗ We recommend that you to have a look at the [Detailed System Requirements](#)^[26] before updating to the current version! Officially supported operating systems, browsers, and other requirements may have changed since version 9.

Update from PRTG Network Monitor 7 or 8

- ❗ We strongly recommend that you perform a clean install of the latest PRTG version instead of updating from an existing PRTG 7 or 8!

If you use PRTG 7 or 8 now, you have to update PRTG to intermediate versions first to ensure all data is carried over correctly. You **cannot update to PRTG 15 or later directly** from PRTG 7 or 8!

- We recommend that you first update to the latest PRTG 8 version.
- From the latest PRTG 8 version update to PRTG version 9.
- From PRTG 9, update to both [intermediate versions](#)^[85] 12.4.7.3507 and 16.1.21.1691/1692 and then to the current PRTG version.

Please [contact our technical support](#)^[375] to obtain download links for these PRTG versions. Always keep a proper backup of your configuration and monitoring data!

Updating from PRTG 7 or 8 to Current PRTG Version

- Packet Sniffer (Content) sensors are not supported anymore. Existing sensors of this type will automatically be switched to Packet Sniffer (Header) sensors after the update. As a benefit, you can now also sniff IPv6 traffic.
- Internet Explorer 8 is no longer supported for access to the PRTG Ajax web interface.
- You may experience a slow [Enterprise Console](#)^[343] (former 'Windows GUI') due to different reasons.
- When installing a failover node on top of an existing stand-alone PRTG 7, 8, 9, 12, or 13+ installation, the configuration cannot be kept and is written to a backup folder. Then, the new cluster configuration is received from the master node of the cluster. As all nodes work with the same configuration, a failover node's old configuration and monitoring data can no longer be used. If you want to keep a configuration of PRTG 7, please install the master node on top of the old installation and use other servers for the failover node installations.
- Since PRTG 9 the SNMP sensors use the **IPv4 Outgoing IP** set for the probe service (this setting was formerly ignored by those sensors, using the **auto** setting instead). If you experience failing sensors, please check the setting in the [probe settings](#)^[371].
- If you have (manually) configured the PRTG probe or PRTG core service to run under a different Windows user account (for example, for successful internet access through an ISA server firewall), please apply the respective Windows user account for the "PRTGProbeService" and/or "PRTGCoreService" anew after installing the current PRTG version.

- System Requirements for the PRTG core server and probes: please have a look at our latest [Detailed System Requirements](#)^[26].
 - If you use the default data path in your PRTG setup, it will be changed automatically. Up to version 8 all data was stored in a sub folder reflecting a PRTG version number (v7 or v8). As of version 9 this sub folder is omitted, and data is stored directly at `%ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor`. During setup, all data will be moved to the new directory. If you use a custom data path it will not be changed.
 - Up to version 8 all data in the registry was stored in a sub key reflecting a PRTG version number (v7 or v8). As of version 9 this sub key is omitted, and registry data is stored directly under the key `HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor` (on 32-bit systems) respectively `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor` (on 64-bit systems). During setup, all existing registry values will be moved to the new key.
-  We strongly recommend that you have a look at the [Detailed System Requirements](#)^[26] before updating to the current version! Officially supported operating systems, browsers, and other requirements may have changed since version 8.

Updating from PRTG 7 to Current PRTG Version

- Regarding custom sensors, the interpretation of returned values is handled more strictly as of PRTG 8. If you use custom sensors with PRTG 7, these may not work with the current PRTG version if they do not fully apply to the [API definition](#)^[366].

Update from Older PRTG Products

For all other predecessor products, a direct data import into the current version is not possible.

If you have been using IPCheck 5 or PRTG Traffic Grapher 6, please perform a clean installation of PRTG Network Monitor and set up your configuration anew. Using the [Auto-Discovery](#)^[282] in PRTG is the easiest way to quickly configure a monitoring of your entire network.

 For more information, see the manual section [Quick Start Guide](#)^[46].

More

Knowledge Base: How do I backup all data and configuration of my PRTG installation?

- <https://kb.paessler.com/en/topic/523>

Knowledge Base: Customizing and Re-Branding the PRTG Web Interface

- <https://kb.paessler.com/en/topic/33>

Knowledge Base: What about my web interface customizations as of PRTG 13.2.3?

- <https://kb.paessler.com/en/topic/44703>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Part 4: Installing the Software | 2 Update From Previous Versions

Knowledge Base: Updating from Version 7, 8, 9 or 12? Read this important message!

- <https://kb.paessler.com/en/topic/35563>

Knowledge Base: Can I update from PRTG Traffic Grapher or IP Check 5 to the current PRTG version?

- <https://kb.paessler.com/en/topic/26553>

Knowledge Base: What does error code PE251 mean?

- <https://kb.paessler.com/en/topic/65764>

Knowledge Base: The signature of my PRTG server is not valid. What can I do?

- <https://kb.paessler.com/en/topic/66308>

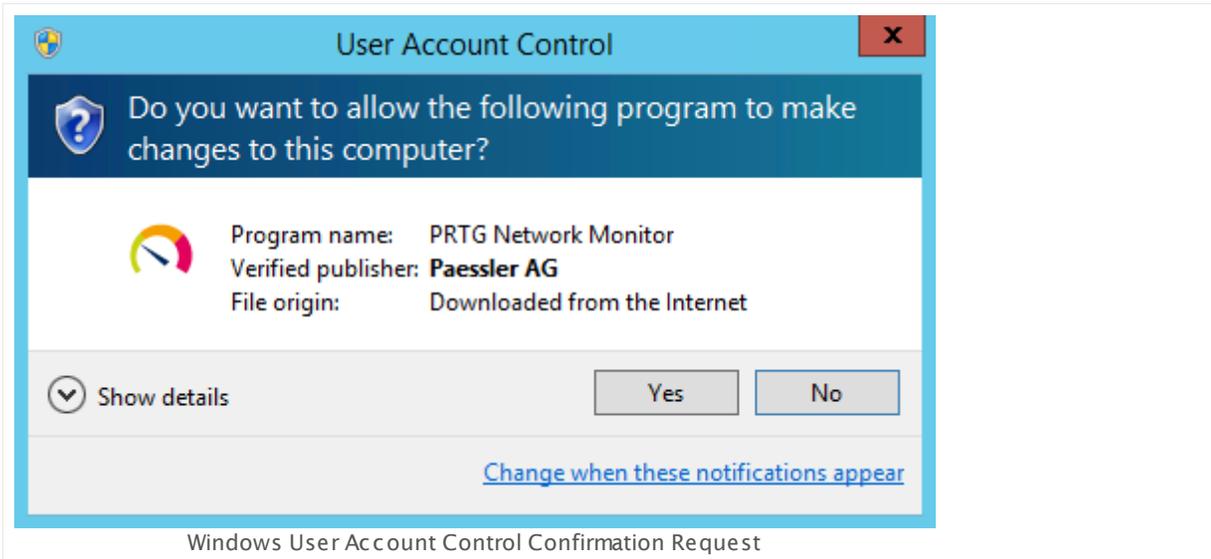
Knowledge Base: Which sensor types do you remove from PRTG and what are the alternatives?

- <https://kb.paessler.com/en/topic/68227>

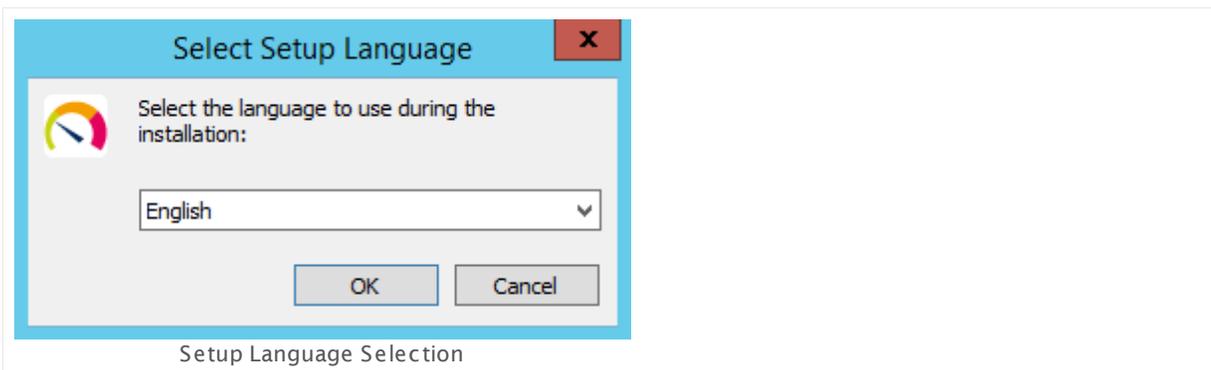
4.3 Install a PRTG Core Server

Installing PRTG Network Monitor is easy and works like other Windows-based applications. To install PRTG, run the installation setup program from the ZIP file that you have downloaded.

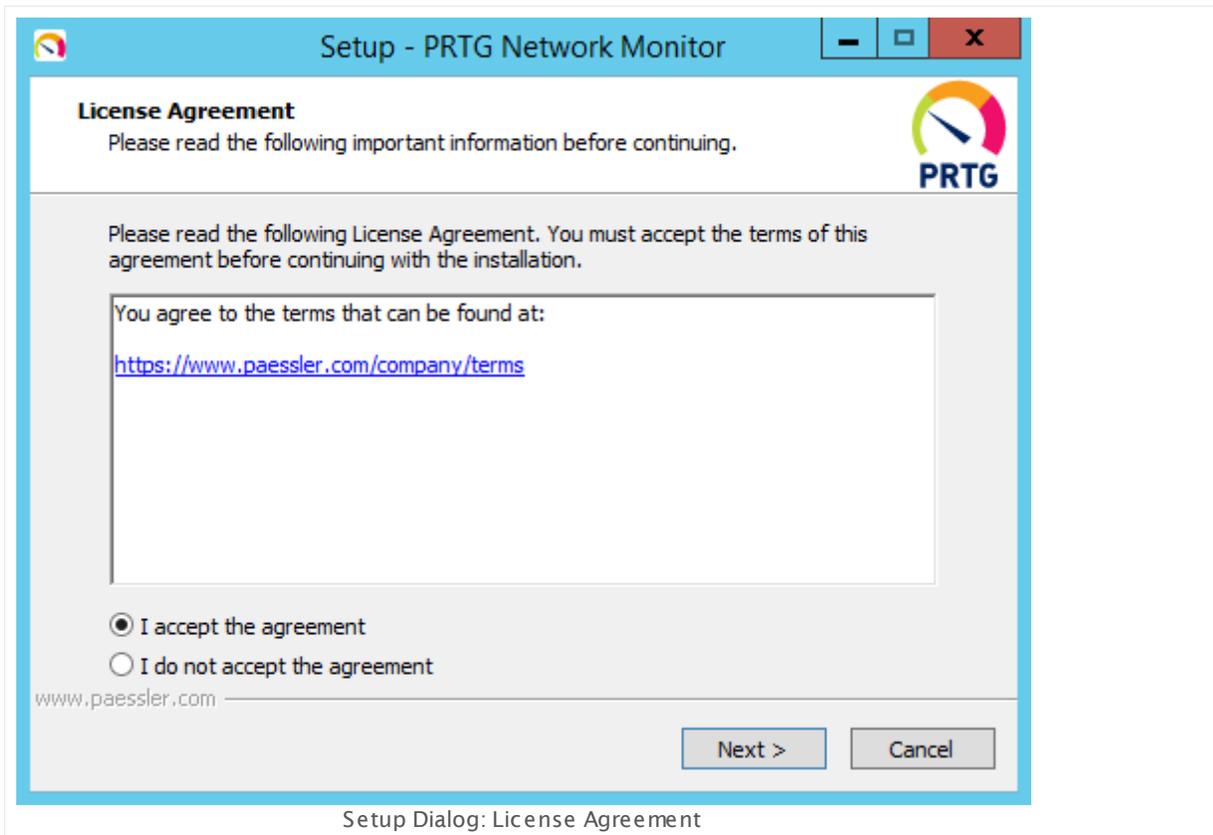
☁ This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.



Confirm the question of the Windows **User Account Control** with **Yes** to allow the program to install. The PRTG installation dialog will guide you through the installation process.



Select a language for the program and click the **OK** button. The available language options depend on both your Windows version and the setup file.



Accept the [license agreement](https://www.paessler.com/company/terms) and click **Next**.

Your Email Address
The following information is required to continue with the installation

Whenever the sensors in your installation discover outages or suspicious values, PRTG can send notifications to alert you. Please enter your email address to make sure you receive these important system alerts. Paessler will also use this address to provide support.

Your Email Address:
john.q.public@example.com

We protect your personal data!
[See our privacy policy for more information.](#)

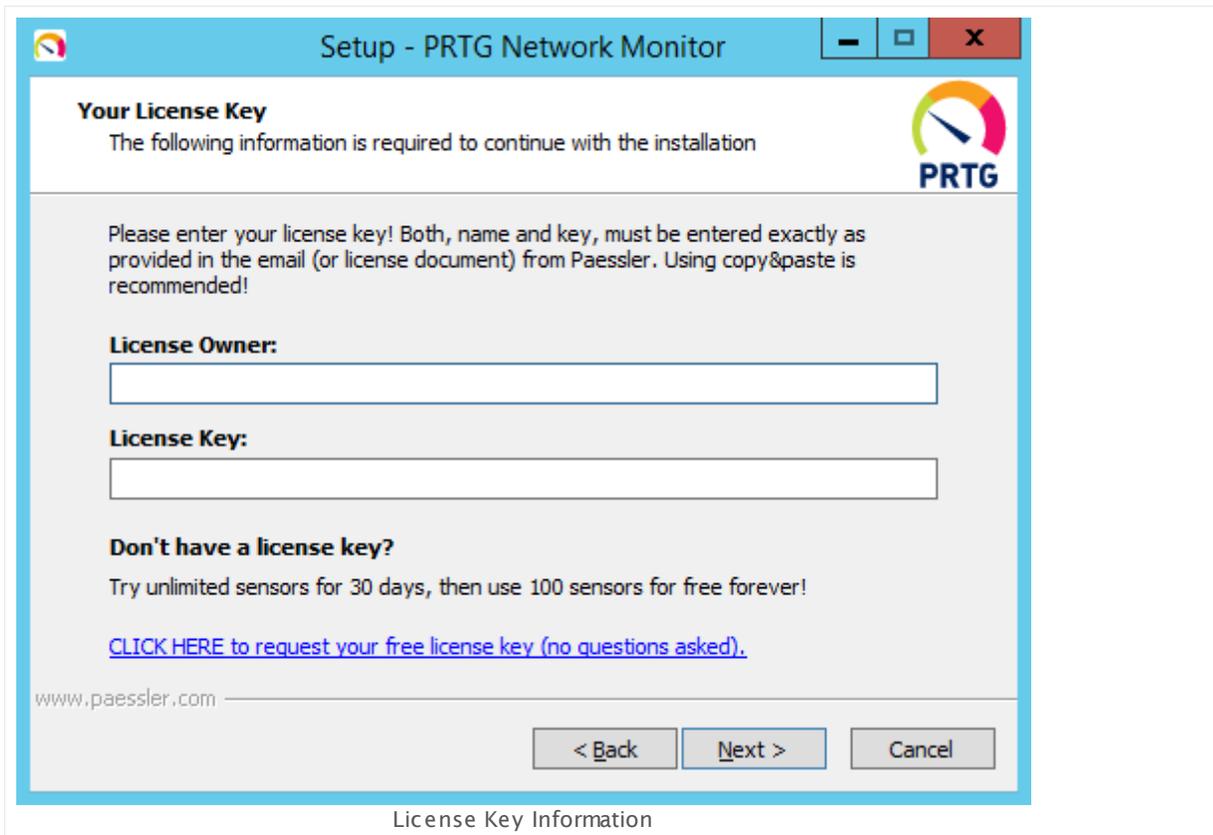
www.paessler.com

< Back Next > Cancel

Administrator Email Address

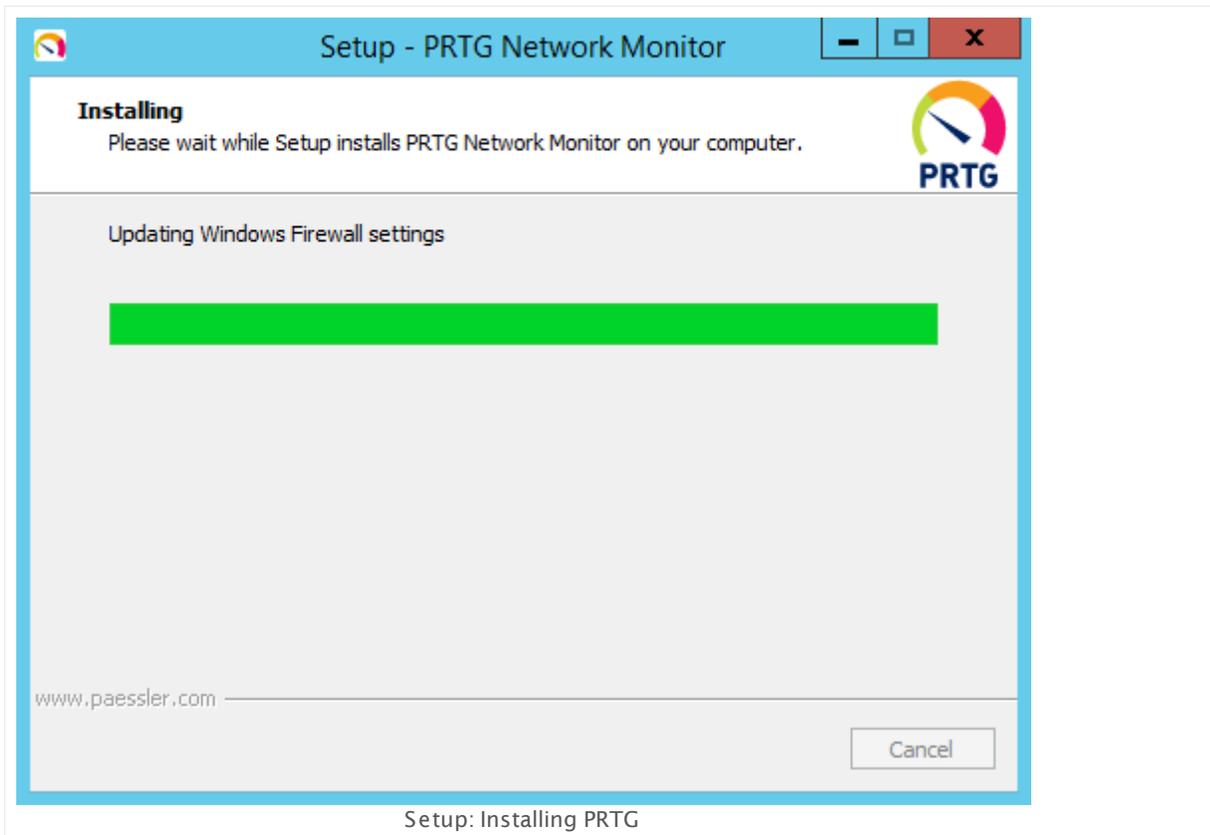
Enter a valid email address. Your PRTG server will send important and urgent system alerts to this address. Click the **Next** button to continue.

 For more information on how we process your personal data, see our [Privacy Policy](#).



Enter your license information. You have to provide the **License Name** and the **License Key** exactly as you received it in the email or license document from us, the Paessler AG. We recommend that you use copy&paste to avoid typos. Click **Next** to confirm.

i You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you [change your license key](#)⁹⁶.



After installation, PRTG opens the [Ajax Web Interface](#)^[166] in your system's default browser. Make sure there is Google Chrome 67 or later (recommended), Mozilla Firefox 61 or later, or Microsoft Internet Explorer 11 available on the system, and set as default browser (see [System Requirements](#)^[23]).

! In certain cases, antivirus software like Windows Defender interfere with the PRTG installer. This might cause high CPU load on the PRTG server, which might prevent a successful installation of PRTG. Please temporarily disable Windows Defender and other antivirus software if you have issues installing PRTG.

Enter License Information

PRTG will validate your license information during the install process by connecting to the activation server. If you have entered incorrect license information before, PRTG will ask you to re-enter a correct License Name and key. Please enter both **License Name** and **License Key** exactly as received from Paessler. We recommend that you use copy&paste to avoid typing mistakes.

+ For more details, see [Enter a License Key](#)^[96].

If you think that you have correctly entered your license information but get a **License Invalid** message, please contact sales@paessler.com.

i You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you [change your license key](#)⁹⁶.

More

Knowledge Base: How can I establish a secure web interface connection to PRTG?

- <https://kb.paessler.com/en/topic/273>

Knowledge Base: PRTG blocks port 80 although I'm using SSL on port 443. How to free port 80?

- <https://kb.paessler.com/en/topic/5373>

License Agreement

- <https://www.paessler.com/company/terms>

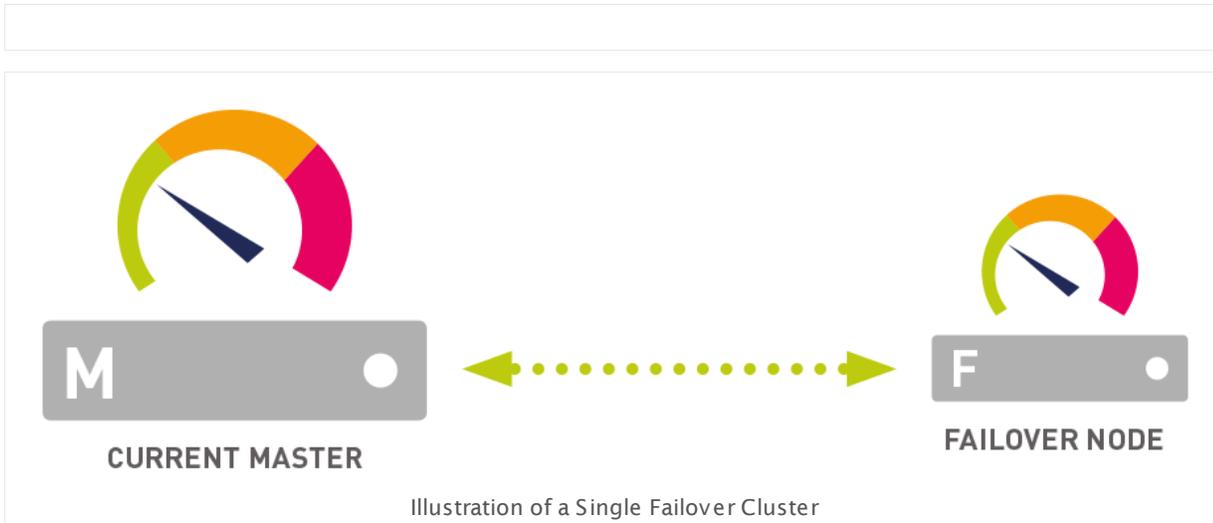
Privacy Policy

- <https://www.paessler.com/company/privacypolicy>

4.4 Install a PRTG Cluster

PRTG offers single failover clustering in all licenses—even using the freeware edition. A single failover cluster consists of two servers ("Current Master" Node and "Failover Node"), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data. You can run a cluster with up to 5 nodes.

☁ This feature is not available in PRTG hosted by Paessler.



📖 For detailed information, see [Failover Cluster Configuration](#)³⁷²⁰.

More

Knowledge Base: What's the Clustering Feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

4.5 Enter a License Key

A license key for PRTG Network Monitor consists of the **License Name** and a **License Key**. The key is a string that consists of 8 blocks with 5 characters each.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

Your Personal License Information

You have received the **License Name** and the **License Key** from Paessler via email or in a license document on [Paessler shop](#). Please copy this information and insert it when PRTG asks you to about your license information in the setup dialog.

 You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you [change your license key](#)^[96].

 For the Trial and Freeware editions, you will receive the required license information on the Paessler webpage when you download the trial or freeware version of PRTG. For a commercial edition, use your commercial license information.

EXAMPLE OF LICENSE INFORMATION

License Name: **John Q. Public**
License Key: **P1000-FFSEJ-ZHGRD-UR1CS-U73FG-G645F-YVF1D-H8323**

During the setup process, PRTG will ask you to enter your license information. Please use copy and paste to fill out the form in the installer dialog.

- **Trial/Freeware license key:** When entering a Trial license key, you can experience unlimited functionality of PRTG during the 30-day trial period. Your installation automatically switches to a Freeware Edition afterwards. For details about how to get your free Trial edition, please see [Download PRTG](#)^[81] section.
- **Commercial license key:** You can only enter this key if you have purchased a commercial license. Your installation allows the number of sensors according to your [license](#)^[21].

Change License Key

Usually you do not need to enter a key manually after the installation to activate it, because PRTG asks for it during the install process. However, there are still scenarios where you need to change your key and activate this license. You have to provide your commercial license key, for example, if you have purchased a PRTG Commercial Edition and want to upgrade your running PRTG Freeware or Trial installation, or if you upgrade an existing commercial license to a higher edition.

- To enter a new license key, log in to the [PRTG web interface](#)^[166].
- Choose **Setup | License** from the [main menu bar](#)^[263].

Part 4: Installing the Software | 5 Enter a License Key

- <https://www.paessler.com/support/videos/prtg-basics/sensor-count>

Knowledge Base: How do I upgrade to a higher edition of PRTG?

- <https://kb.paessler.com/en/topic/4193>

4.6 Activate the Product

PRTG will activate your license automatically via the internet during the install process. Only if PRTG cannot connect to the internet directly and so cannot access the activation server, will you have to activate your license manually.

You have to complete the product activation process once to use PRTG, otherwise it will not run. Do not forget to activate your commercial license when you want to upgrade your trial or freeware installation!

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

Online Activation

Usually you do not need to enter a key manually after the installation to activate it, because PRTG asks for it during the install process. However, there are still scenarios where you need to change your key and activate this license. You have to provide your commercial license key, for example, if you have purchased a PRTG Commercial Edition and want to upgrade your running PRTG Freeware or Trial installation, or if you upgrade an existing commercial license to a higher edition.

- To enter a new license key, log in to the [PRTG web interface](#) ¹⁶⁶.
- Choose **Setup | License** from the [main menu bar](#) ²⁶³.
- Click **Change License Key**.
- The **Update Your License** page appears where you can activate your new license.
- Choose the activation type **Automatic (online activation with optional HTTP proxy)** if your PRTG server can connect to the internet.
 - ❗ Without internet access, you have to choose **Manual (offline activation)**. The activation process works a bit different in this case and requires manual interactions.
- Provide your license information and click **Update License**.
- PRTG will connect to the Paessler activation server via SSL on port 443 and validate your license.
- If everything works fine, you will see the message **Activation was successful** as **License Status** on top of the page.

 For details, see manual section [PRTG Status—Licensing Status and Settings: Update Your License](#) ³⁴¹⁶.

❗ The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, please configure it in [Step 3: Activate](#) ³⁴¹⁷ on the **Update Your License** page. If activation fails, you can also try an offline activation.

 This option is not available in PRTG hosted by Paessler.

Offline Activation

If there is no internet connection available, you have to activate PRTG manually.

 This option is not available in PRTG hosted by Paessler.

- In the [PRTG web interface](#)¹⁶⁶, choose **Set up | License** from the [main menu bar](#)²⁶³.
- Click **Change License Key**.
- The **Update Your License** page appears where you can activate your license.
- Choose the activation type **Manual (offline activation)** if your PRTG server cannot connect to the internet.
- Provide your license information and follow the instructions in [step 3](#)³⁴¹⁶ and [step 4](#)³⁴¹⁶.
- Click **Update License**.
- If everything works fine, you will see the message **Activation was successful** as **License Status** on top of the page.

 For details, see manual section [PRTG Status—Licensing Status and Settings: Update Your License](#)³⁴¹⁶.

 If your PRTG server is offline, you need to manually activate your license after you have renewed your maintenance. This ensures you can enjoy the benefits of an active maintenance like the possibility to install updates. Your maintenance information has to fit the PRTG installer, so accomplish your offline activation before you install an update.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- <https://kb.paessler.com/en/topic/32513>

4.7 Install a PRTG Remote Probe

- ✳ Why are remote probes helpful for monitoring with PRTG? Because you can extend your monitoring.
 - Remote probes allow you to monitor different sub-networks that are separated by a firewall from your PRTG on premises core server and to keep an eye on remote locations. You can install [one or more remote probes](#)^[3703].
 - Remote probes are useful if you want to distribute monitoring load by taking it from the system running the PRTG core server and putting it on one or more remote probe machines.
 - You will need a remote probe if you want to monitor your local network using a PRTG hosted by Paessler instance.
 - Remote probes may be suitable monitoring components in several individual scenarios that depend on your custom network setup.

All you need is a computer on which you can install your remote probe. See also the [System Requirements for PRTG Remote Probes](#)^[23].

Steps to Go

To install a PRTG Remote Probe, follow these steps:

- [1. Prepare the PRTG Core Server](#)^[102]: only required for PRTG on premises 
- [2. Download the Remote Probe Installer](#)^[104]: start here if you use PRTG hosted by Paessler 
- [3. Install the Remote Probe](#)^[105]
- [4. Approve New Probe and Start Monitoring](#)^[107]

 Your PRTG on premises or PRTG hosted by Paessler installations already include a [local probe](#)^[3744] or [hosted probe](#)^[3745] on the PRTG core server. This is why you cannot additionally install a remote probe on your core server system.

 PRTG updates remote probes automatically, but in rare cases a manual probe update is required. You will receive a [ToDo ticket](#)^[230] in this case. Please follow the steps [below](#)^[104] to manually update a remote probe.

 If you have issues after the installation, see this section: [Debugging Remote Probe Connection Problems](#)^[109]

 Do you run PRTG in a cluster? Then mind this [important note](#)^[103].

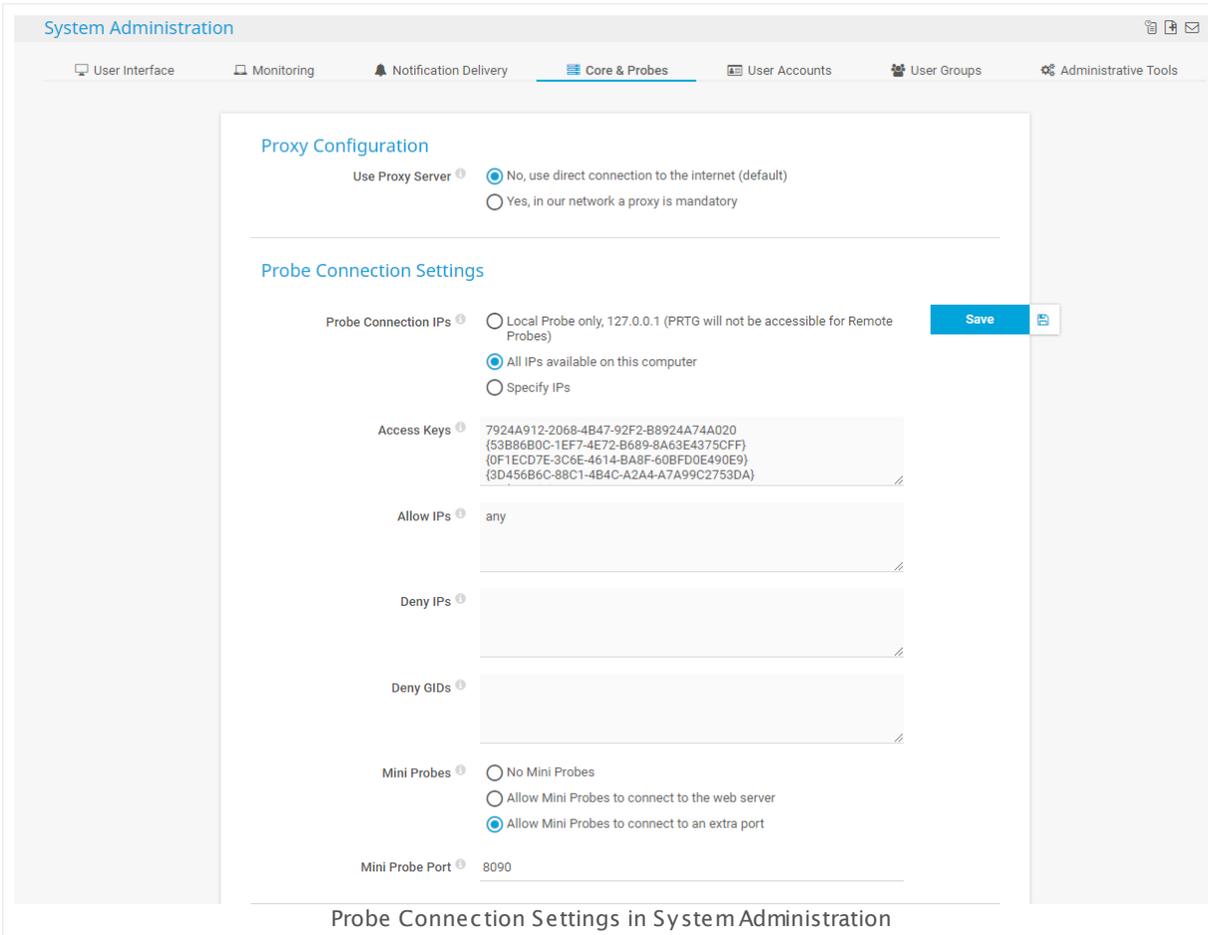
1. Prepare the PRTG Core Server

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

So, if you use PRTG hosted by Paessler, you can start with [2. Download the Remote Probe Installer from the PRTG Web Interface](#)^[104] right away.

 Because your remote probe needs to connect to your PRTG core server, PRTG needs to accept incoming remote probe connections. So, on PRTG on premises, prepare your PRTG server first when you want to install the remote probe.

Edit the relevant settings in [System Administration—Core & Probes](#)^[338]. From the main menu in the [PRTG web interface](#)^[168], select **Set up | System Administration | Core & Probes** to access the probes settings and go to the **Probe Connection Settings**.



The screenshot shows the 'System Administration' interface with the 'Core & Probes' tab selected. The 'Proxy Configuration' section has 'Use Proxy Server' set to 'No, use direct connection to the internet (default)'. The 'Probe Connection Settings' section is expanded, showing 'Probe Connection IPs' set to 'All IPs available on this computer'. Other settings include 'Access Keys' (a long alphanumeric string), 'Allow IPs' set to 'any', 'Deny IPs' and 'Deny GIDs' (empty), 'Mini Probes' set to 'Allow Mini Probes to connect to an extra port', and 'Mini Probe Port' set to '8090'. A 'Save' button is visible next to the 'Probe Connection IPs' setting.

System Administration

User Interface | Monitoring | Notification Delivery | **Core & Probes** | User Accounts | User Groups | Administrative Tools

Proxy Configuration

Use Proxy Server ¹ No, use direct connection to the internet (default)
 Yes, in our network a proxy is mandatory

Probe Connection Settings

Probe Connection IPs ¹ Local Probe only, 127.0.0.1 (PRTG will not be accessible for Remote Probes) **Save** 
 All IPs available on this computer
 Specify IPs

Access Keys ¹ 7924A912-2068-4B47-92F2-B8924A74A020
 (53B86B0C-1EF7-4E72-B689-8A63E4375CFF)
 (0F1ECD7E-3C6E-4614-BA8F-60BFD0E490E9)
 (3D456B6C-88C1-4B4C-A2A4-A7A99C2753DA)

Allow IPs ¹ any

Deny IPs ¹

Deny GIDs ¹

Mini Probes ¹ No Mini Probes
 Allow Mini Probes to connect to the web server
 Allow Mini Probes to connect to an extra port

Mini Probe Port ¹ 8090

Probe Connection Settings in System Administration

Step 1: Probe Connection IPs

By default, a core server accepts connections from the **Local Probe only** (IP address **127.0.0.1**). This setting is the most secure setting, but it does not allow any remote probe to connect to your PRTG core server.

To accept remote probes, choose one of the following settings:

- **All IPs available on this computer:** Any IP on your core server system accepts incoming probe connections.
- **Specify IPs:** Specify selected IP addresses that accept incoming connections.

Step 2: Allow IPs

In the **Allow IPs** field, you can enter the IP address of the computer you want to install a remote probe on. To make things easier, you can also enter the word **any**. Any will set the PRTG core server to accept remote probes connecting from any IP address.

- ❗ If you use **any**, make sure you write the word in lower case only! Any other variations will not be valid!

Changing other settings is not required. For details about the fields for **Access Keys**, **Deny IPs**, and **Deny GIDs** see section [System Administration—Core & Probes](#).

When you are done, click **Save** to save your settings.

- ❗ If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#), or of [PRTG Apps for Mobile Network Monitoring](#) will be disconnected and reconnected.

- ❗ To edit the core-probe connection settings you can also use the [PRTG Administration Tool](#) on your core server.

PRTG Cluster and Remote Probes Outside the LAN

- ⚠ If you use the [Clustering](#) feature of PRTG and you want to run remote probes outside your local network, you have to make sure your cluster nodes and the addresses they use are reachable from the outside! Check your cluster node settings under [System Administration—Cluster](#) before installing a remote probe outside your local network. Enter addresses (DNS names or IPs) that are valid for both cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

- 📄 If you already have a remote probe installed outside your LAN and the probe is disconnected because of this, please follow these steps:

1. Uninstall the current remote probe.
2. Update the [cluster node settings](#) with addresses that are reachable from outside your LAN.
3. Restart your PRTG core servers.

4. Install the remote probe again. It will then obtain the IP address or DNS name entries that it can reach.

See also section [Failover Cluster Configuration—Remote Probes in Cluster](#).

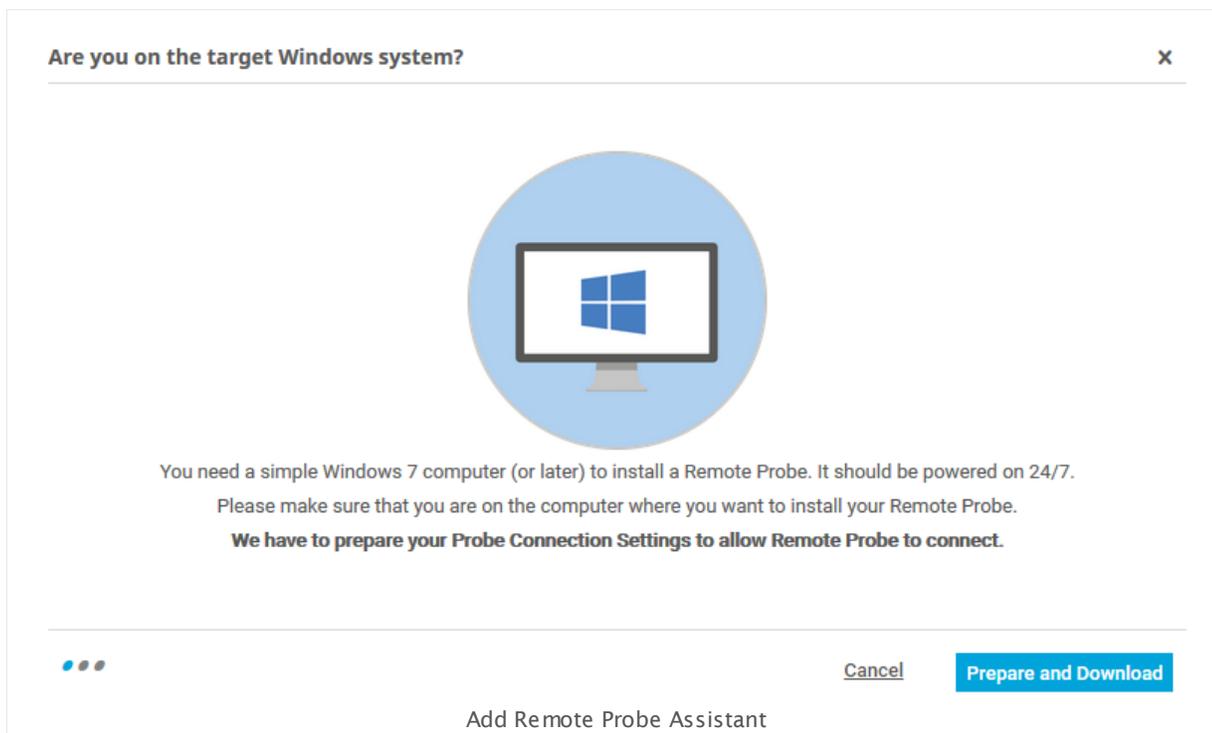
2. Download the Remote Probe Installer from the PRTG Web Interface

On the computer on which you want to install a remote probe, [log in to the PRTG web interface](#). From the [main menu bar](#), select **Set up | Downloads and Tools | Remote Probe Installer**. Click **Add Remote Probe** to start the installation assistant. In the appearing dialog window, click **Prepare and Install** to start the download. Save the setup program to your local disk.

The **Add Remote Probe** button is also available in the device tree.

Using the installation approach with the assistant, PRTG will guide you through the install process. If you **Download the Remote Probe Installer directly**, you have to install the remote probe without the assistant.

If you connect your remote probe to a PRTG on premises instance, [prepare](#) your **Probe Connection Settings** first.

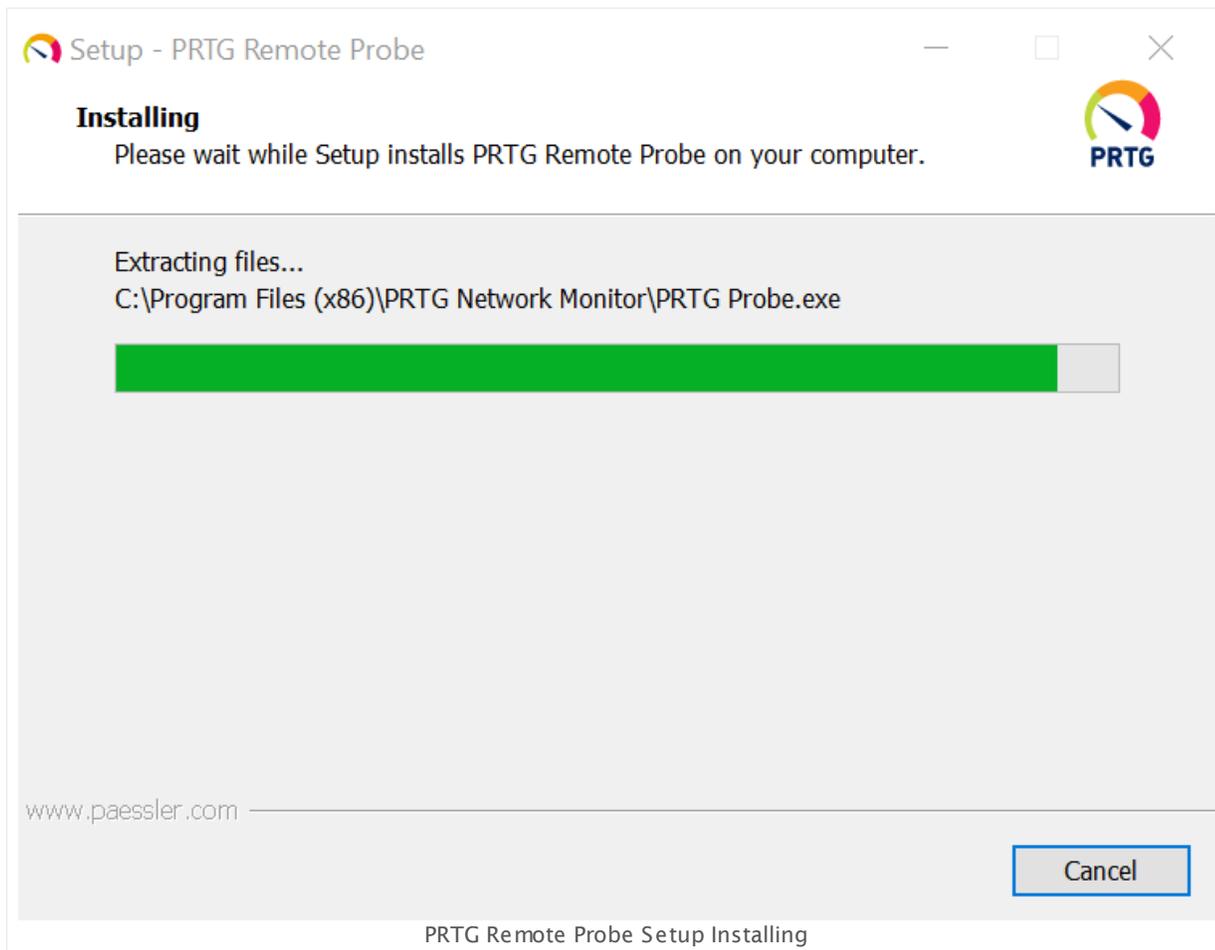


The version numbers of core and probe services must match. PRTG updates probes automatically when a new version is installed on the PRTG core server. If PRTG advises you to update your remote probe manually, open a web browser on your remote computer and download the remote probe installer as described in this manual section.

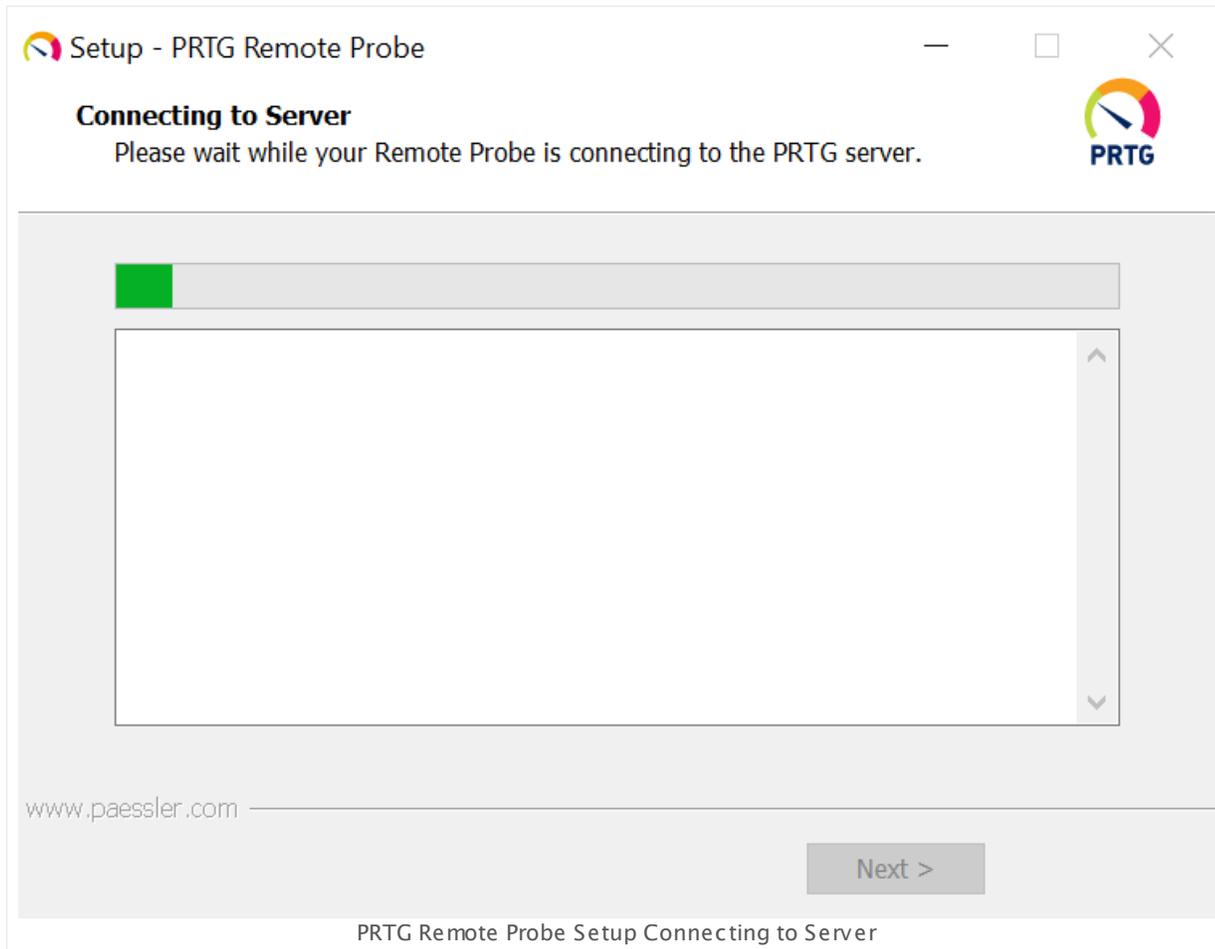
- i** The PRTG core system already includes a local probe or hosted probe service. This is why you cannot additionally install a remote probe on that system.

3. Install the Remote Probe

- Execute the setup program that you have just downloaded.
- Confirm the Windows User Account Control dialog with **Yes** to allow the installation. The usual software installation wizard will guide you through the installation process.
- Click **Install** to start the installation process of your remote probe.

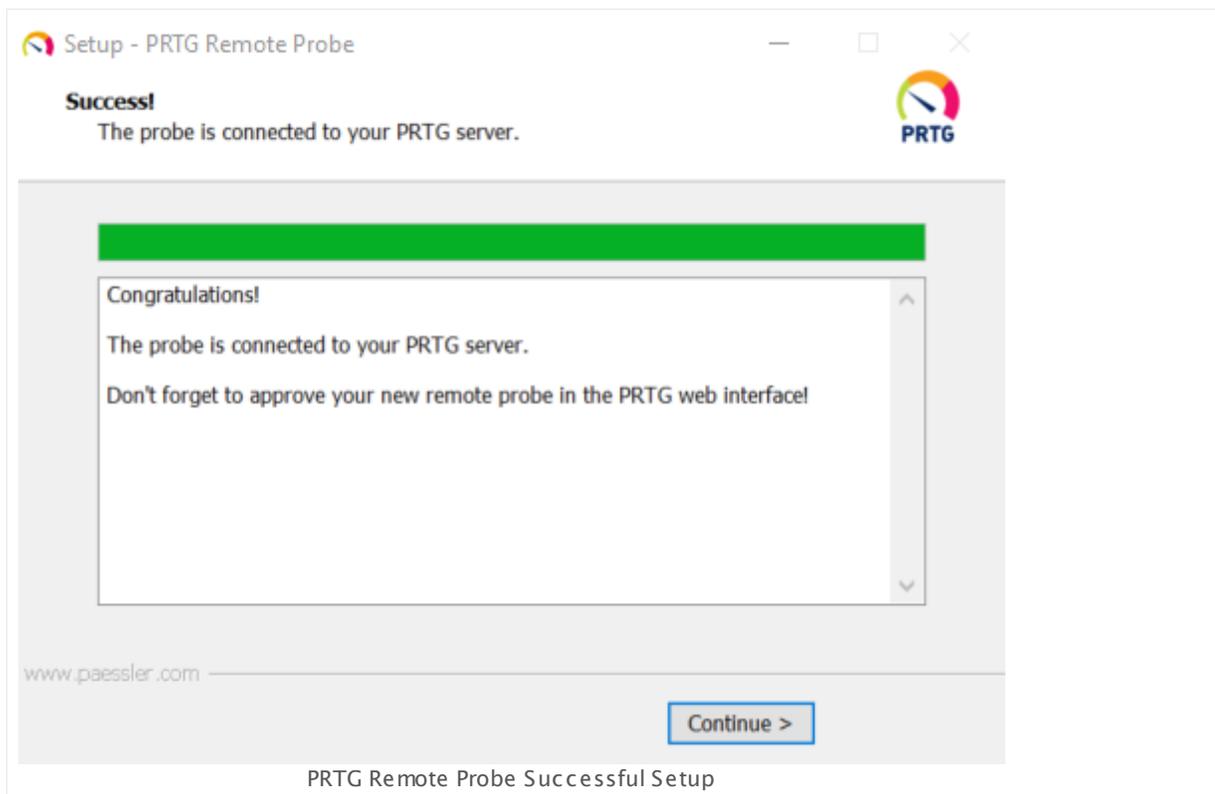


Please wait until the installation is completed. The remote probe will automatically connect to your PRTG core server.



If the remote probe successfully connects to your PRTG core server, you can complete the setup of your new remote probe.

i To allow your new remote probe to connect to a PRTG hosted by Paessler instance, PRTG automatically sets the **Allow IPs** field in [System Administration—Core & Probes](#) to **any**. You can also use **any** for PRTG on premises, but we recommend that you use this setting in intranets only. If **any** is not an option for you, cancel it in the **Allow IPs** field and enter the IP address of your remote probe instead.



Click **Continue** to finish the remote probe installation.

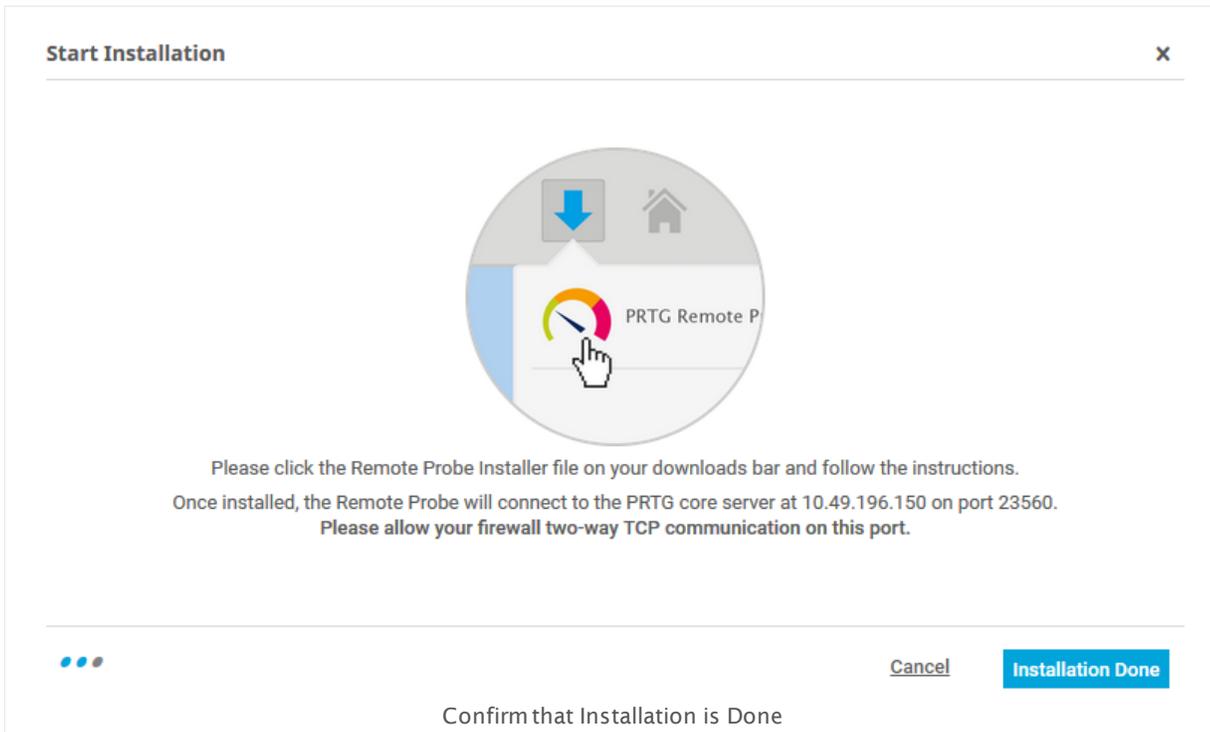
Finally, click **Finish** to exit the installation wizard. The remote probe is now installed on your computer as a Windows service.

Approve the New Probe and Start Monitoring

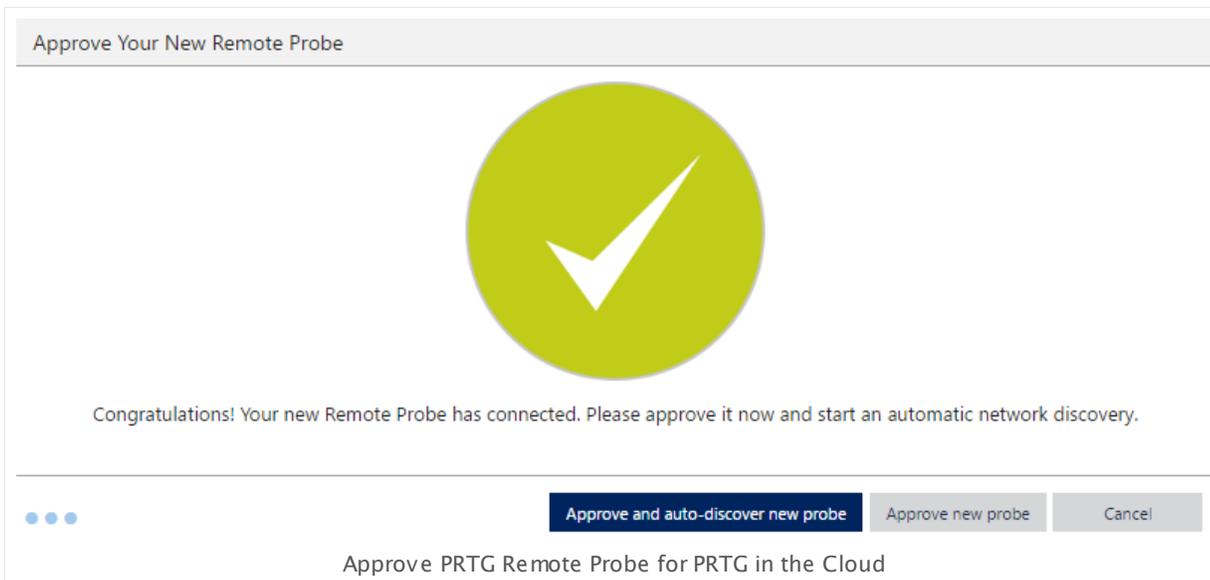
Remember to log in to the PRTG web interface, confirm that the installation is done, and acknowledge your new remote probe!

In the installation assistant, click **Installation Done**.

Part 4: Installing the Software | 7 Install a PRTG Remote Probe



☁ If you successfully installed the remote probe from a PRTG hosted by Paessler installation, you will see the following dialog box.

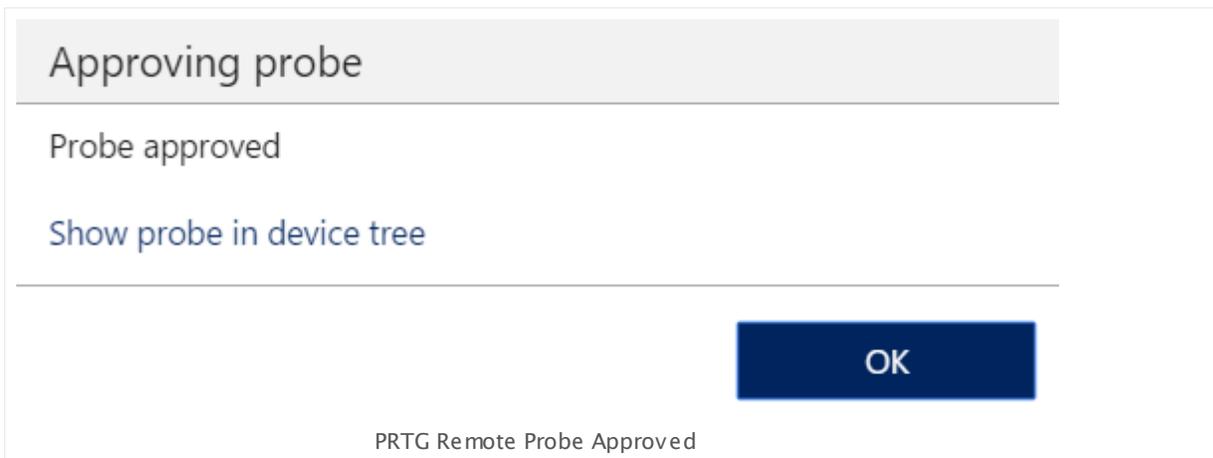


Click **Approve and auto-discover new probe** to include your new remote probe device and network in your device tree and to start the PRTG [auto-discovery](#)²⁸². It helps you discover devices and automatically create suitable sensors. Optionally, you can also choose to only approve your remote probe without starting an auto-discovery by clicking **Approve new probe**. The probe now appears as a new object in your device tree.

For unwanted probe connections, you can click **Deny new probe**. Note that this does not uninstall the remote probe, but only prohibits the probe from connecting to the PRTG core server.

i If you deny or remove a remote probe, PRTG will automatically add this device's global ID (GID) to the **Deny GIDs list** in [System Administration—Core & Probes](#)^[3368]. Future probe connections from this device will be denied automatically.

i Denying the remote probe in the PRTG device tree does **not** uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.



In the **Approving probe** dialog, click **OK** to exit the dialog, or click **Show probe in device tree** to open the new probe in the device tree directly.

Once approved, PRTG automatically creates a set of sensors for the probe to ensure you can detect bottle-necks on the probe system immediately. We recommend that you keep these sensors. You can now create groups, devices, and sensors for monitoring via the new probe.

i You do not have to approve remote probes after updates.

When a new probe connects to the core server for the first time, you will receive a new [ToDo ticket](#)^[2301] in the PRTG ticket system.

Debugging Remote Probe Connection Problems

If you have trouble with your core probe connection, make sure that you meet the following requirements:

- The IP address of the computer on which you want to install a remote probe is not listed in the **Deny IPs** field in [System Administration—Core & Probes](#)^[3368].
- On your PRTG core server side, the default port **23560** for probe connections is not blocked by firewall rules, and, on the probe side, the TCP port **23560** is open for outgoing connections as well.

Part 4: Installing the Software | 7 Install a PRTG Remote Probe

 If you need to set a different port (not recommended), see this Knowledge Base article: [How can I customize PRTG's ports for core-probe-connections?](#)

- You can also take a look at the probe's logfiles. The probe process writes logfiles with a file name in the format **PRTG Probe Log (x).log**. Open the one with the most recent date.

For a correct connection the probe log should look similar to this:

```
11/6/2017 1:21:58 PM PRTG Probe V17.4.36.3253
11/6/2017 1:21:58 PM System time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
11/6/2017 1:21:58 PM libeay32.dll=1.0.2.11
11/6/2017 1:21:58 PM ssleay32.dll=1.0.2.11
11/6/2017 1:21:58 PM PRTG Probe "example-DNS" starting on "example-DNS" (GID={AAAA1111-22BB-33CC-DD44-EEEE
11/6/2017 1:21:58 PM Memory Manager: NexusMM4
11/6/2017 1:21:58 PM OS: Microsoft Windows 10 Enterprise (10.0 Build 15063), 4 CPUs (Quad x64 Model 78 Ste
11/6/2017 1:21:58 PM Data Path: C:\ProgramData\Paessler\PRTG Network Monitor\
11/6/2017 1:21:58 PM System Path: C:\Program Files (x86)\PRTG Network Monitor\
11/6/2017 1:21:58 PM Local IP: 0.0.0.0
11/6/2017 1:21:58 PM Core Server IP: example-DNS.exampledomain.com
11/6/2017 1:21:58 PM Core Server Port: 23560
11/6/2017 1:21:58 PM SSL Enabled
11/6/2017 1:21:58 PM Probe GID: {AAAA1111-22BB-33CC-DD44-EEEEEE555555}
[...]
11/6/2017 1:21:58 PM Start Connection
11/6/2017 1:21:58 PM Start Done
11/6/2017 1:21:58 PM (14608):Initializing WMIConnectionPool
11/6/2017 1:21:58 PM (14608):WMIConnectionPool maximum number of concurrrent establishing is set to: 20
11/6/2017 1:22:03 PM Connect from to example-DNS.exampledomain.com:23560
11/6/2017 1:22:03 PM TCP connected from 10.49.12.51:55199 to example-DNS.exampledomain.com:23560
11/6/2017 1:22:03 PM State changed to connected (example-DNS.exampledomain.com:23560)
11/6/2017 1:22:03 PM Reconnect
11/6/2017 1:22:04 PM Connected
11/6/2017 1:22:10 PM Send Login
11/6/2017 1:22:10 PM Local: 11/6/2017 1:22:10 PM UTC: 11/6/2017 12:22:10 PM
11/6/2017 1:22:10 PM MarkUnused
11/6/2017 1:22:10 PM Login OK: Welcome to PRTG
```

If the connection fails, for example due to an incorrect **Access Key**, or due to incorrect **IP** settings (see [Prepare the PRTG Core Server](#)^[102]), you will see:

```
11/6/2017 1:42:02 PM Try to connect...
11/6/2017 1:42:02 PM Connected to 10.0.2.167:23560
11/6/2017 1:42:07 PM Login NOT OK: Access key not correct!
```

If you need to adjust any probe settings for the connection to the PRTG core server, use the [PRTG Administration Tool](#)^[3387] on your remote probe system.

Remote Probe Settings in PRTG Administrator

In the **Connection to PRTG Core Server** tab, you can then edit the following settings:

- **Server:** Enter the IP address or DNS name of the core server the remote probe will connect to. If Network Address Translation (NAT) is used, this has to be the IP address that is externally visible, because the remote probe will connect from outside your network.
- **Probe Access Key** and **Confirm Access Key:** Enter the access key that the probe will send to the core server. This access key has to be defined on the PRTG core server in [System Administration—Core & Probes](#)^[3388]. Make sure the key phrases match exactly.

Remember to always click **Save & Close** to confirm your settings and to (re)start the probe service.

 For more detailed information about these settings, see section [PRTG Administration Tool](#)

More

Knowledge Base: How can I customize PRTG's ports for core-probe-connections?

- <https://kb.paessler.com/en/topic/65084>

4.8 Install the Enterprise Console

The Enterprise Console is already included in a [PRTG core server installation](#)^[89] (PRTG on premises only) You can install additional Enterprise Consoles on other computers.

☁ PRTG hosted by Paessler does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

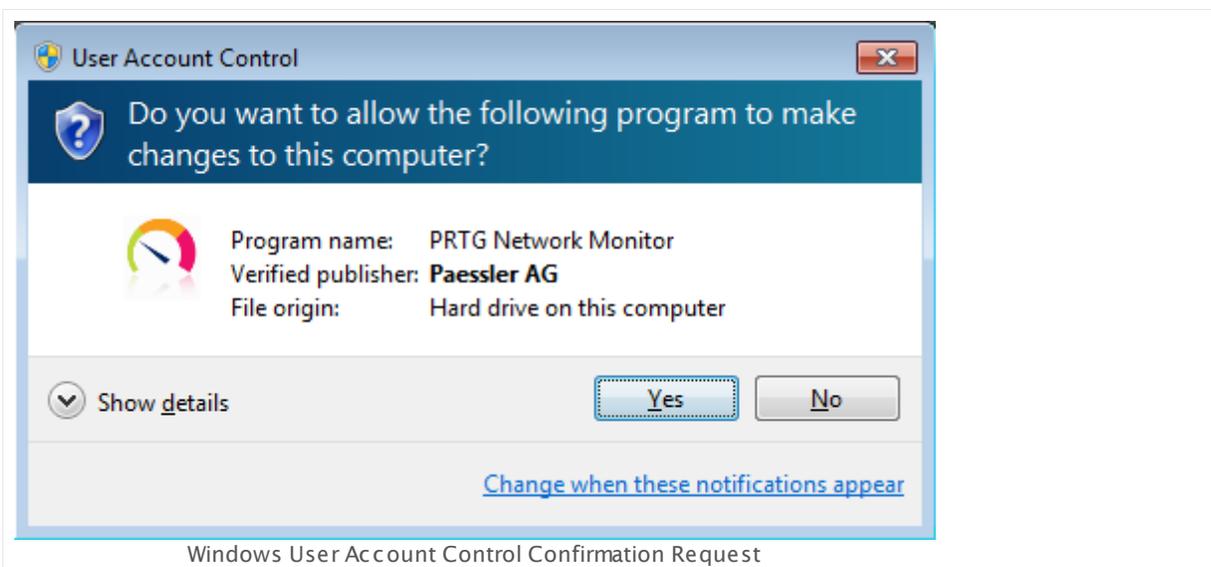
Download Enterprise Console from the Web Interface

The version of the Enterprise Console (EC) has to match the PRTG core server version you want to connect to. It can connect to a PRTG server where the third entry in the version number is equal to the third entry of the EC version number. For example, EC version 15.1.16.2023 can connect to any PRTG server with version 15.1.16.xxxx.

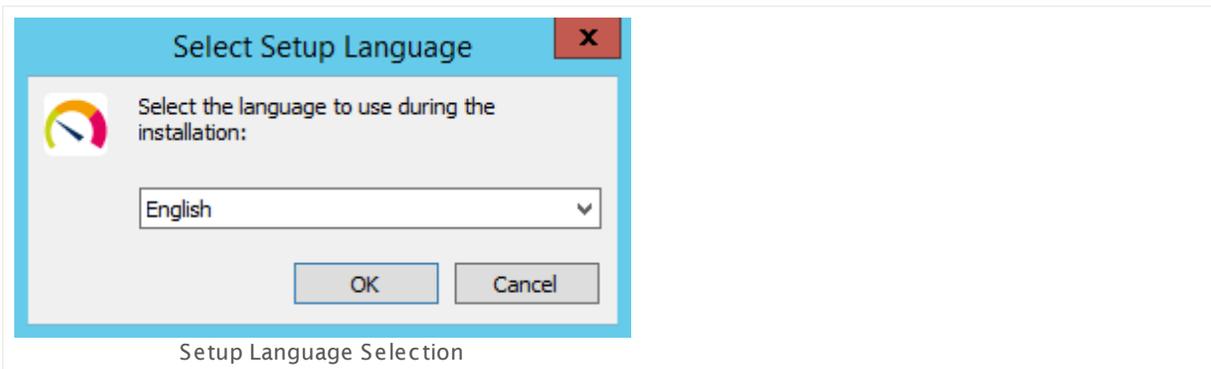
1. From the computer you want to install the Enterprise Console on, connect to the [Ajax](#)^[166] web interface of PRTG.
2. On the [login screen](#)^[168] of the web interface, enter login name and password and click **Download Client Software (optional, for Windows, iOS, Android)**.
3. You will see the [downloads page](#)^[3420] where you can download the EC.
4. Click **Download: PRTG Enterprise Console** and save the setup program to the local hard disk drive.

Install Enterprise Console

Execute the setup program `PRTG_Enterprise_Console_Installer.exe` that you have downloaded.



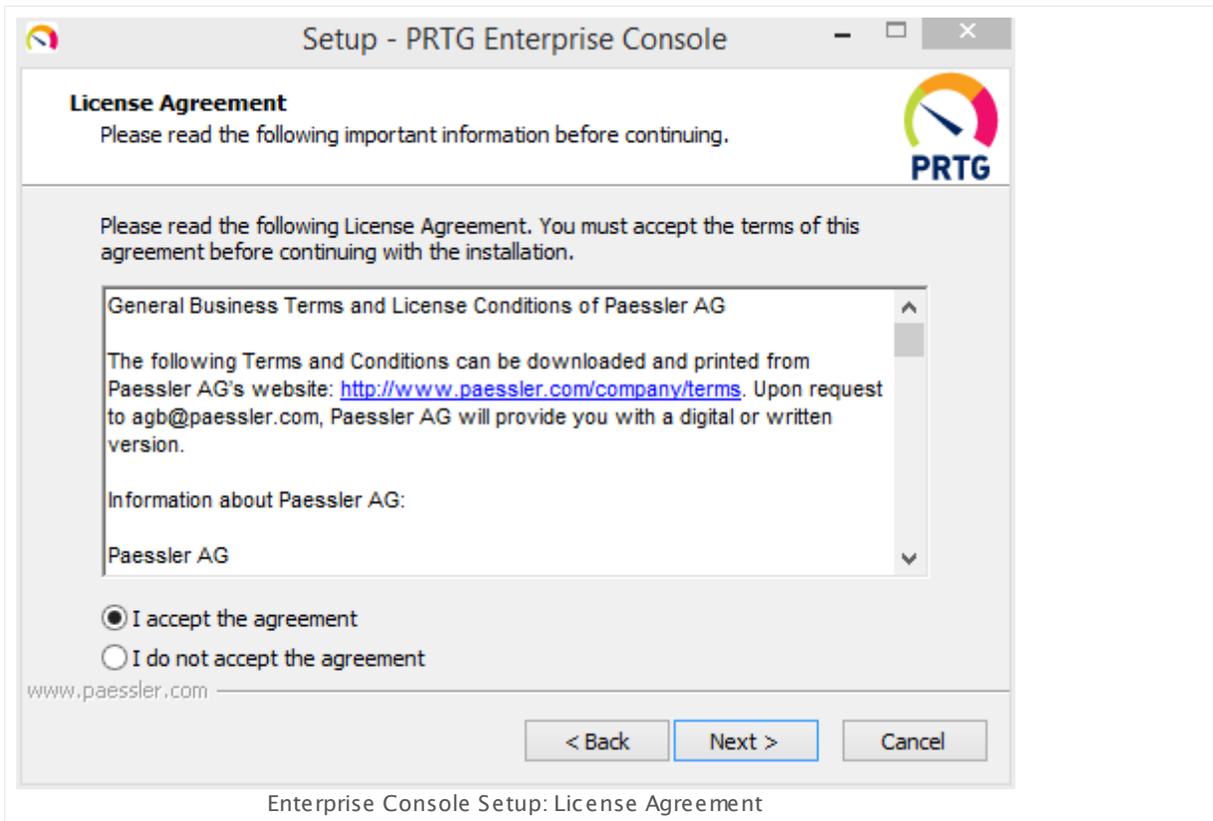
Confirm the question of the **Windows User Account Control** with **Yes** to allow the program to install. The usual software installation assistant will guide you through the installation process.



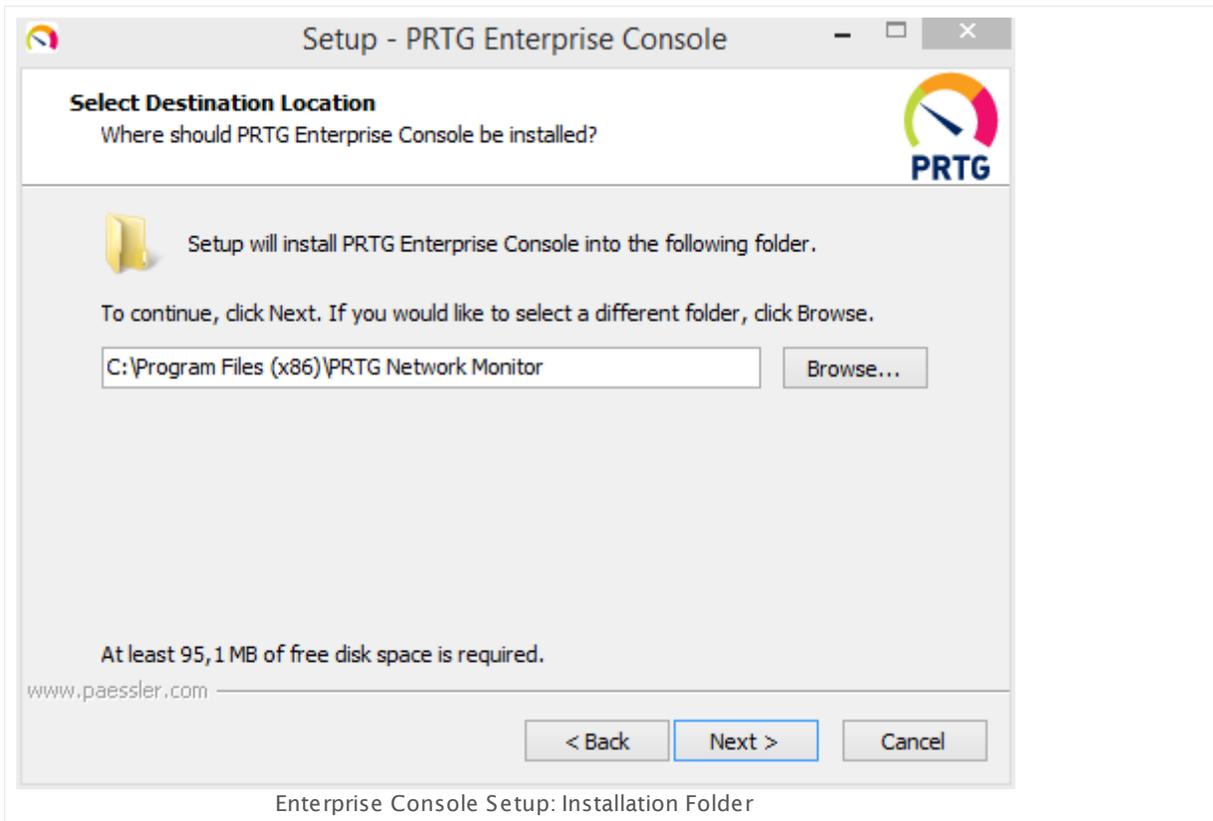
Select a language for the program and click the **OK** button. The available language options depend on both your Windows version and the setup file.



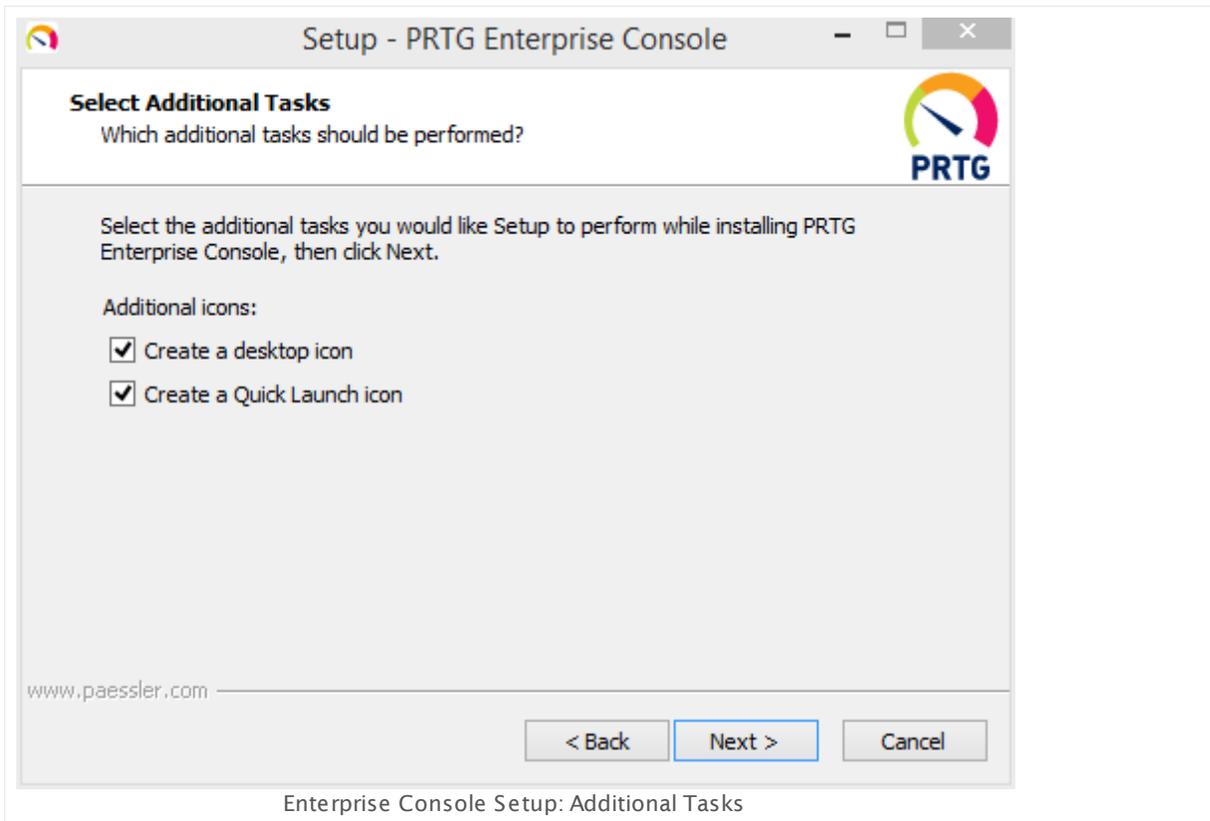
Click **Next** to walk through the wizard.



After accepting the license agreement, you can choose the folder you wish to install the software in. We recommend that you use the default value.



Select the start icons you want to create for the Enterprise Console. We recommend that you use the default value.



Click **Next** to copy the necessary files to the disk of your computer.

After installation, click **Finish** to start the Enterprise Console. Enter [the settings for the connection to your PRTG server](#) ³⁴³¹ in the appearing dialog.



More

See the section [Enterprise Console](#) ³⁴³⁰ for more information on how to use this Graphical User Interface (GUI).

4.9 Uninstall PRTG Products

The uninstall process has six steps—regardless of if you are uninstalling an entire PRTG Network Monitor installation, a single Enterprise Console installation, or a PRTG Remote Probe installation. Use the Windows uninstall routines to remove the PRTG software from your system.

Step 1

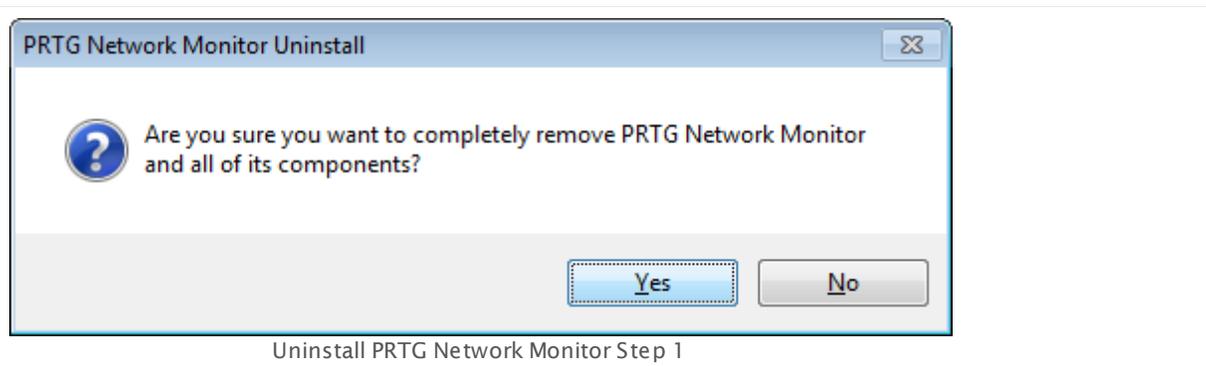
From the Windows Start Menu, run **Uninstall PRTG Network Monitor**, **Uninstall PRTG Enterprise Console**, or **Uninstall PRTG Remote Probe**, or open your Windows Control Panel and choose the desired entry in the **Programs** section. Depending on the installed products, not all uninstall programs are available.

Step 2

If asked, confirm the question of the Windows User Account Control with **Yes** to allow the program to uninstall. The software uninstall dialog will guide you through the uninstall process.

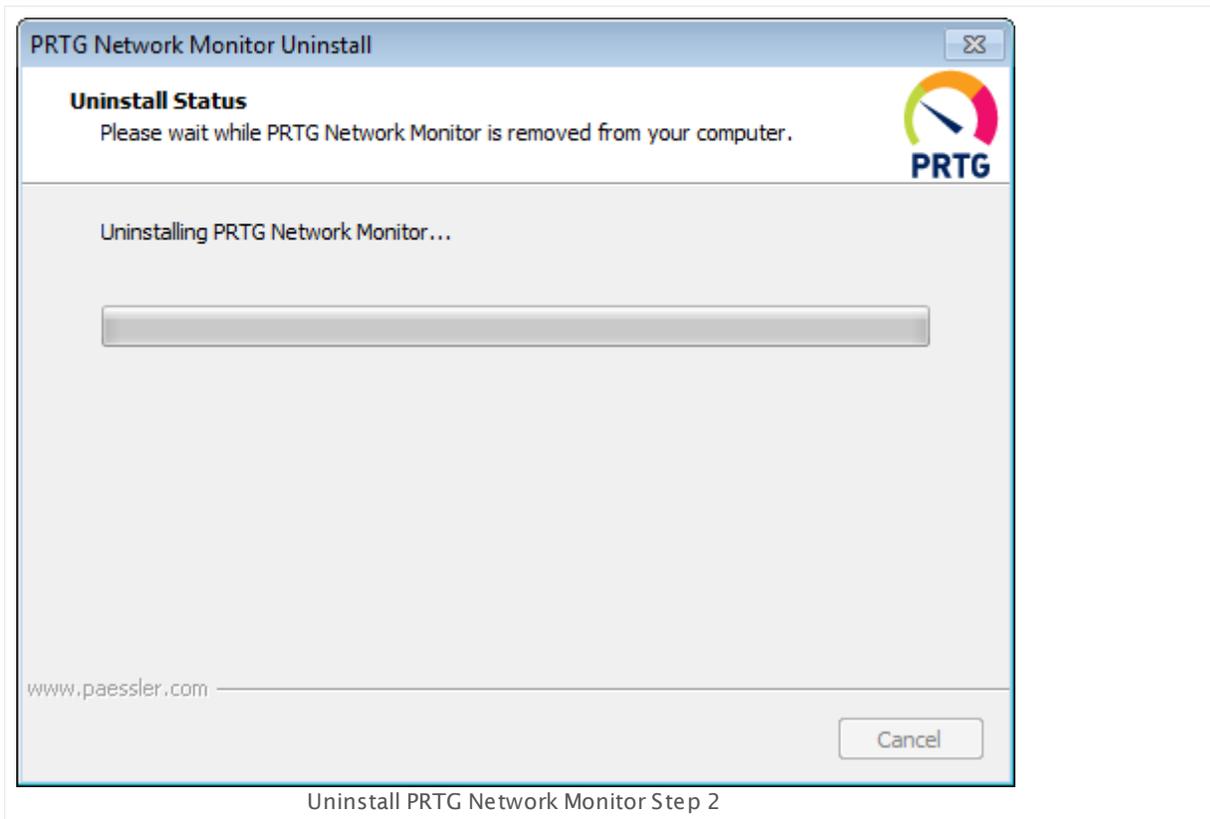
Step 3

Confirm the removal of the software by clicking the **Yes** button.



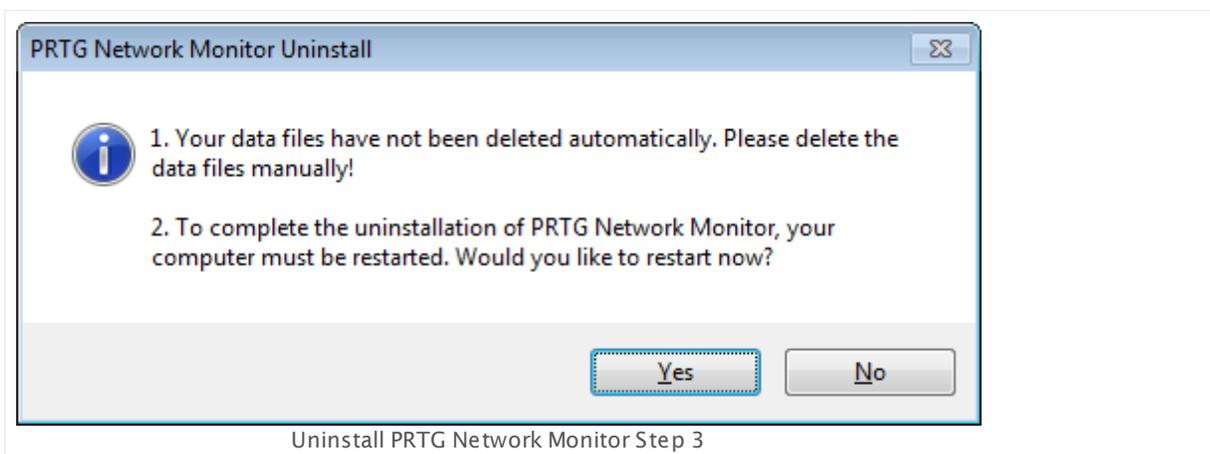
Step 4

Wait while the software is being removed.



Step 5

Confirm a system restart by clicking the **Yes** button.



Step 6

After system restart, the software is removed, but there still will be some custom data in the PRTG program folder. If you have uninstalled an entire PRTG Network Monitor installation or a remote probe installation, your monitoring data is still stored on the system. To completely remove all PRTG data, delete the **PRTG Network Monitor** program folder as well as the **Paessler\PRTG Network Monitor** folder in your data path.

 For more information on where the data is stored see the [Data Storage](#)  section.

More

Knowledge Base: Can we remotely and silently uninstall a Remote Probe?

- <https://kb.paessler.com/en/topic/27383>

Part 5

Understanding Basic Concepts

5 Understanding Basic Concepts

There is a number of basic concepts that are essential for understanding the functionality and ease of use of PRTG Network Monitor. We have made using our software as easy as possible. Setting it up for the first start and getting first monitoring results happens almost [automatically](#) ^[52].

Nevertheless, there are some basic principles we would like to explain to you. Please read these sections carefully to understand the underlying workflow like architecture of the monitoring system, hierarchy of objects, settings inheritance, and notifying. You will be able to enhance your monitoring experience permanently as soon as you know the basic principles of PRTG!

Understanding Basic Concepts—Topics

- [Architecture and User Interfaces](#) ^[125]
- [Clustering](#) ^[130]
- [Object Hierarchy](#) ^[133]
- [Inheritance of Settings](#) ^[137]
- [Tags](#) ^[139]
- [Dependencies](#) ^[141]
- [Scheduling](#) ^[142]
- [Notifying](#) ^[143]
- [Data Reporting](#) ^[162]
- [User Access Rights](#) ^[158]
- [IPv6](#) ^[163]

5.1 Architecture and User Interfaces

What is PRTG Network Monitor and how does it work? If you are new to PRTG or simply want to check if you got PRTG right, you are welcome on this page! We are glad to introduce PRTG and its components to you.

Overview

You can classify the PRTG Network Monitor components in three main categories: System parts, control interfaces, and a basic administration interface.

TYPE	PART OF PRTG
System Parts	<p>Core Server¹²⁶</p> <p>This is the central part of a PRTG installation and includes data storage, web server, report engine, a notification system, and more. The core server is configured as a Windows service that runs permanently.</p>
	<p>Probe(s)¹²⁶</p> <p>The part of PRTG that performs the actual monitoring. There are local probes, remote probes, and cluster probes in PRTG on premises, and there are hosted probes and remote probes in PRTG hosted by Paessler. All monitoring data is forwarded to the central core server. Probes are configured as Windows services that run permanently.</p>
	<p> We assume that all computers on which the PRTG core server with its local probe or any remote probes run are secure. It is every administrator's responsibility to make sure that only authorized persons can access these machines. For this reason we highly recommend that you use dedicated machines for your PRTG system parts.</p>
User Interfaces	<p>PRTG Web Interface¹⁶⁶</p> <p>The Ajax-based web interface is used for configuration of devices and sensors, as well as for the review of monitoring results. Also system administration and user management are configured here.</p>
	<p>Enterprise Console³⁴³⁰</p> <p>A native Windows application as alternative to the web interface to manage your monitoring. With the Enterprise Console, you can connect to different independent PRTG core server installations and review their data at a glance!</p>
	<p>PRTG Apps for Mobile Network Monitoring³⁴⁸⁴</p> <p>Monitor your network on the go with PRTG and apps for iOS and Android.</p>

TYPE	PART OF PRTG
System Administration Program	<p>PRTG Administration Tool on Core Server System³⁵⁶¹  </p> <p>Used to configure basic core server settings in PRTG on premises, such as administrator login, web server IPs and port, probe connection settings, cluster mode, system language, and more.</p> <p>PRTG Administration Tool on Remote Probe System³⁵⁸⁷ </p> <p>Used to configure basic probe settings such as name of the probe, IP and server connection settings, and more.</p>

Core Server

The core server is the heart of your PRTG system and performs the following processes:

- Configuration management for monitoring objects (for example, servers, workstations, printers, switches, routers, virtual machines, and many more)
- Management and configuration of the connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generator and scheduler
- User account management
- Data purging (culling data that is older than 365 days, for example)
- Web server and API server

In a PRTG on premises [cluster](#)¹³⁰¹, the current master node is responsible for all of these tasks.

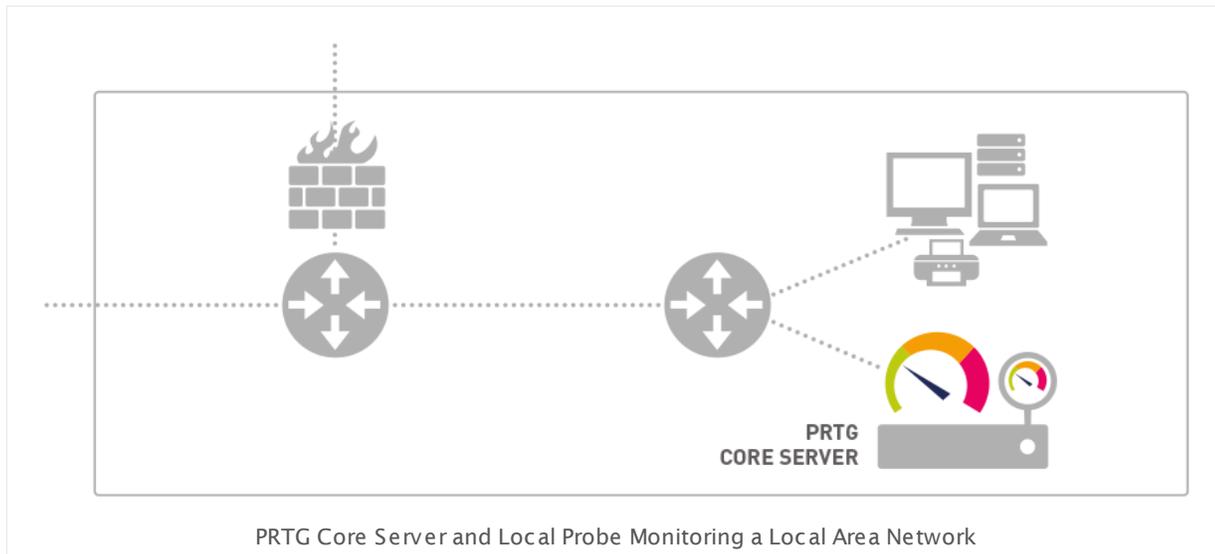
The built-in, fast, and secure web server (no additional IIS or Apache is required) supports HTTP as well as secure HTTPS (via SSL). It serves the web interface when you access it via a browser and also answers PRTG Application Programming Interface (API) calls (for example, for user scripts or the Enterprise Console).

-  Core server and probe(s) are configured as Windows services that are permanently run by the Windows system without the requirement for a logged-in user.

Probe(s)

On a probe, PRTG performs the actual monitoring via the sensors created on a device (for example, computer, router, server, firewall). The probe receives its configuration from the core server, runs the monitoring processes, and delivers monitoring results back to the core server.

- On every system running a PRTG on premises core server, there is always a local probe running on the same machine.
- ☁ In PRTG hosted by Paessler instances, there is always a hosted probe running on the PRTG core server system that we host for you.



The actual monitoring is performed by PRTG probe processes that run on one or more computers.

- ⓘ Core server and probe(s) are configured as Windows services that are permanently run by the Windows system without the requirement for a logged-in user.

Local Probe in PRTG on premises

During installation of PRTG on premises, the system automatically creates the **Local Probe**. In a single-probe installation—which is the default setup—the local probe performs all monitoring.

The PRTG on premises core server with the local probe inside the corporate LAN (bottom-right in the figure above) is able to monitor services and servers in the entire Local Area Network (LAN). In PRTG hosted by Paessler you need at least one [remote probe](#)^[101] installation in your network for this purpose.

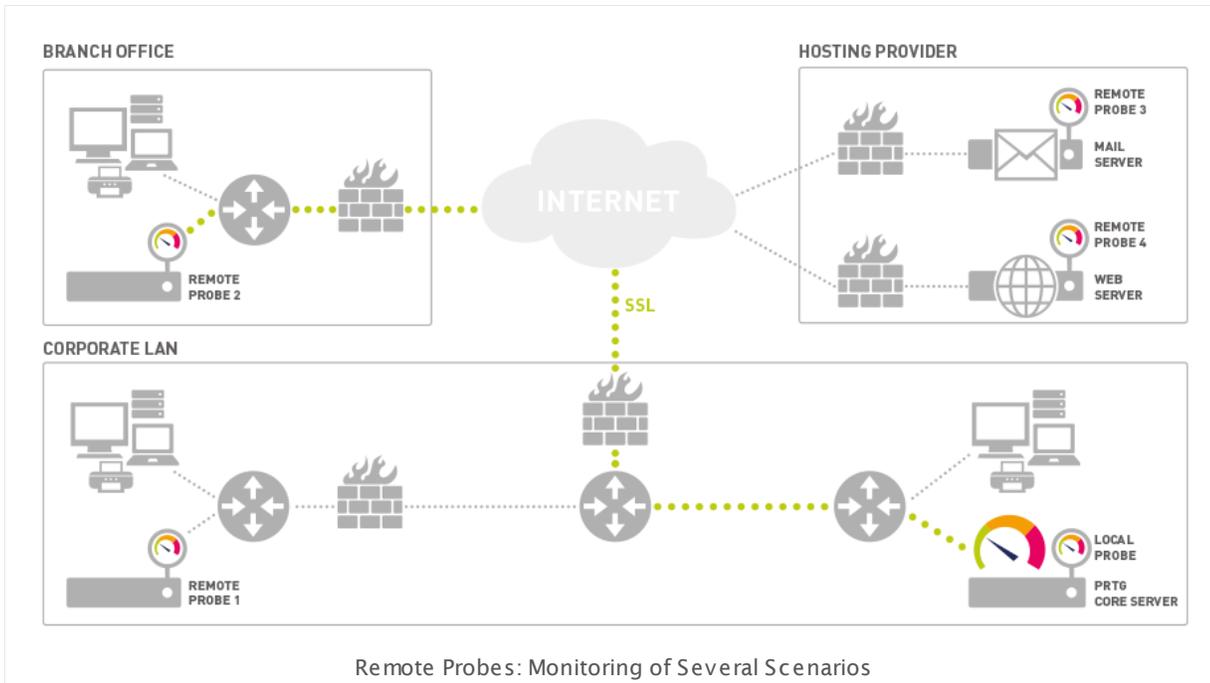
Hosted Probe in PRTG hosted by Paessler

When creating a PRTG hosted by Paessler instance, the system automatically adds the **Hosted Probe**. The hosted probe shows monitoring values of the hosted PRTG instance and is able to monitor devices, servers, and services that are publicly accessible in the internet like, for example, websites. To monitor your Local Area Network (LAN), you need at least one [remote probe](#)^[101] installation in your network. The local probe is not available in PRTG hosted by Paessler.

Remote Probes

You can create additional **Remote Probes** to achieve monitoring of multiple locations, for LAN monitoring with PRTG hosted by Paessler, or for several other scenarios. They use Transport Layer Security (TLS)-secured connections to the core and allow you to securely monitor services and systems inside remote networks that are not openly accessible or are secured by firewalls. For more information, please see [Remote Probes and Multiple Probes](#)^[370].

For more information, see this video tutorial on our website: [Distributed Monitoring with PRTG using Remote Probes](#)



Cluster Probes in PRTG on premises

In a [cluster setup](#)^[130], a cluster probe runs on all nodes. This is the additional **Cluster Probe**. All devices that you create on it are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, also if one of the nodes fails.

Mini Probes in PRTG on premises

PRTG Mini Probes allow you to create small probes on any device (not just on Windows systems). You can implement mini probes to gather monitoring data exactly like you need it and you can create them on any platform.

For more information, see section [Mini Probe API](#)^[360].

System Health Monitoring

PRTG automatically monitors system health of its own core server and of each probe to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors. These include [Core Health](#)^[652] and [Probe Health](#)^[1990], [System Health](#)^[2660], [Cluster Health](#)^[638], [disk free](#)^[2933], and [bandwidth](#)^[2795] sensors for all installed network cards, as well as a [Common SaaS sensor](#)^[644] that checks the availability of widely used SaaS providers.

We recommend that you keep these sensors, but you can optionally remove all except the **Health** sensors. They measure various internal system parameters of the probe system hardware and the probe's internal processes and computes a resulting value. Frequent or repeated values below 100% should be investigated. Please check the [channels](#)^[198] of a particular sensor for details.

More

Looking for a comprehensive PRTG training? PRTG e-learning in 9 modules:

- <https://www.paessler.com/support/training/e-learning>

Video Tutorials: Learn about the PRTG Network Monitor basics on the Paessler video tutorials page.

- <https://www.paessler.com/support/videos/prtg-basics>

Video Tutorial: Distributed Monitoring with PRTG using Remote Probes

- https://www.paessler.com/support/videos/prtg-basics/distributed_monitoring

Video Tutorial: What is a sensor?

- <https://www.paessler.com/support/videos/prtg-basics/what-is-a-sensor>

Video Tutorial: PRTG User Interfaces

- <https://www.paessler.com/support/videos/prtg-basics/user-interfaces>

5.2 Clustering

The main goal of any monitoring solution is to help you reach 100% availability of your IT and network infrastructure and avoid costly downtimes. Because of this, it is necessary to permanently monitor the IT infrastructure and so the objective is to reach true 100% uptime for the monitoring tool. It needs a **high availability mechanism** for this purpose like, for example, **clustering**.

PRTG Network Monitor not only allows you to monitor all your infrastructure with only one tool, but also to monitor it twenty-four hours a day and offers a high availability cluster out-of-the-box. With clustering, the uptime will no longer be degraded by failing connections because of an internet outage at a PRTG server's location, failing hardware, or because of downtime due to a software update for the operating system or PRTG itself.

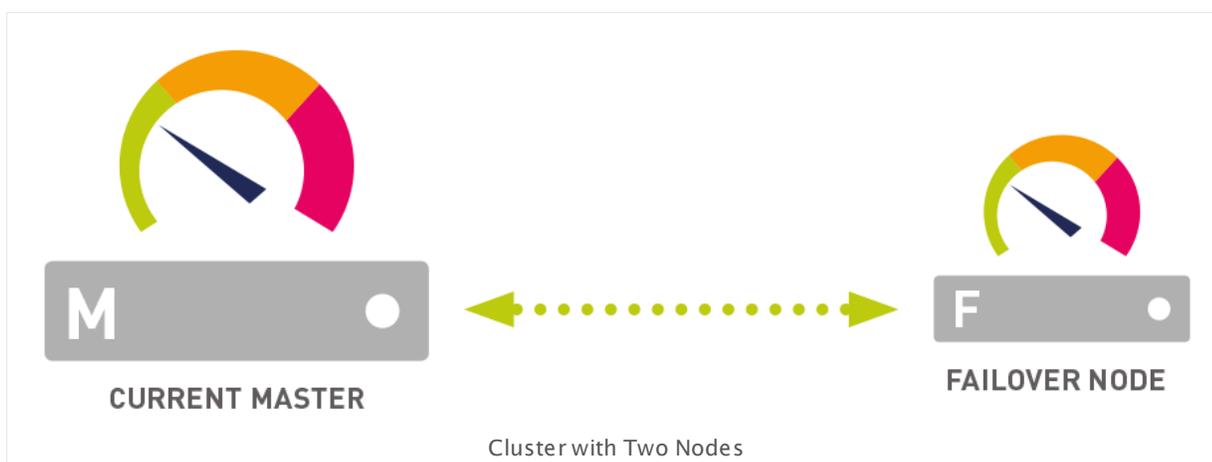
A **PRTG Cluster** consists of two or more [installations of PRTG](#)^[89] that work together to form a high availability monitoring system. All PRTG on premises licenses allow you to have a simple cluster, composed of two PRTG installations working together.

☁ This feature is not available in PRTG hosted by Paessler.

How a PRTG Cluster Works

A PRTG cluster consists of at least two nodes: one **Primary Master Node** and one or more **Failover Nodes**, where up to 4 failover nodes are possible. Each cluster node is simply a full installation of PRTG that could perform the whole monitoring and alerting on its own.

Cluster nodes are connected to each other using two TCP/IP connections. They communicate in both directions and a single node only needs to connect to one other node to integrate into the cluster.



During normal operation you configure devices, sensors, and all other monitoring objects on the **Primary Master** using the [web interface](#)^[166] or [Enterprise Console](#)^[343]. The master node automatically distributes the configuration to all other nodes in real time.

All devices that you create on the **Cluster Probe** are monitored by all nodes in the cluster, so data from different perspectives is available and monitoring for these devices always continues, even if one of the nodes fails. If the **Primary Master** fails, one of the **Failover Nodes** will take over the master role and control the cluster until the master node is back. This ensures a fail-safe monitoring with gapless data.

A PRTG cluster works in **active-active** mode. This means that all cluster nodes are permanently monitoring the network according to the common configuration received from the current master node and each node stores the results into its own database. The storage of monitoring results is also distributed among the cluster. PRTG updates need to be installed on one node only. This node will automatically deploy the new version to all other nodes.

If downtimes or threshold breaches are discovered by one or more nodes, only one installation, either the Primary Master or the Failover Master, will send out notifications (for example, via email, SMS text message, push message). Because of this, the administrator will not be flooded with notifications from all cluster nodes in case failures occur.

 During the outage of a node, it will not be able to collect monitoring data. The data of this single node will show gaps. However, monitoring data for this time span is still available on the other node(s). There is no functionality to actually fill in other nodes' data into those gaps.

Because the monitoring configuration is managed centrally, you can only change it on the master node, but you can review the monitoring results by logging in to the web interface of any of the failover nodes in read-only mode.

If you use [remote probes in a cluster](#)³⁷²³, each probe connects to each node of your cluster and sends the data to all cluster nodes, the current primary master as well as the failover nodes. You can define **Cluster Connectivity** of each probe in the [Probe Administrative Settings](#)³⁷¹.

Performance Considerations for PRTG Cluster

As a consequence of this concept, monitoring traffic and load on the network is multiplied by the number of used cluster nodes. Moreover, the devices on the cluster probe are monitored by all cluster nodes, so you will encounter an increase of monitoring load on these devices.

This will not be a problem for most usage scenarios, but consider the [Detailed System Requirements](#)³⁰. As a rule of thumb, each additional node in the cluster results in dividing the number of sensors that you can use by two.

 More than 5,000 sensors per cluster are not officially supported. Please contact your [presales team](#) if you exceed this limit and see this Knowledge Base article for possible alternatives to a cluster: [Are there alternatives to the PRTG cluster when running a large installation?](#)

Set Up a PRTG Cluster

For detailed information, see [Failover Cluster Configuration](#)³⁷²⁰.

More

Knowledge Base: What's the Clustering Feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

Knowledge Base: In which web interface do I log in if the Master Node fails?

- <https://kb.paessler.com/en/topic/7113>

Knowledge Base: Are there alternatives to the PRTG cluster when running a large installation?

- <https://kb.paessler.com/en/topic/8223>

Video Tutorial: Cluster in PRTG — This is how it works

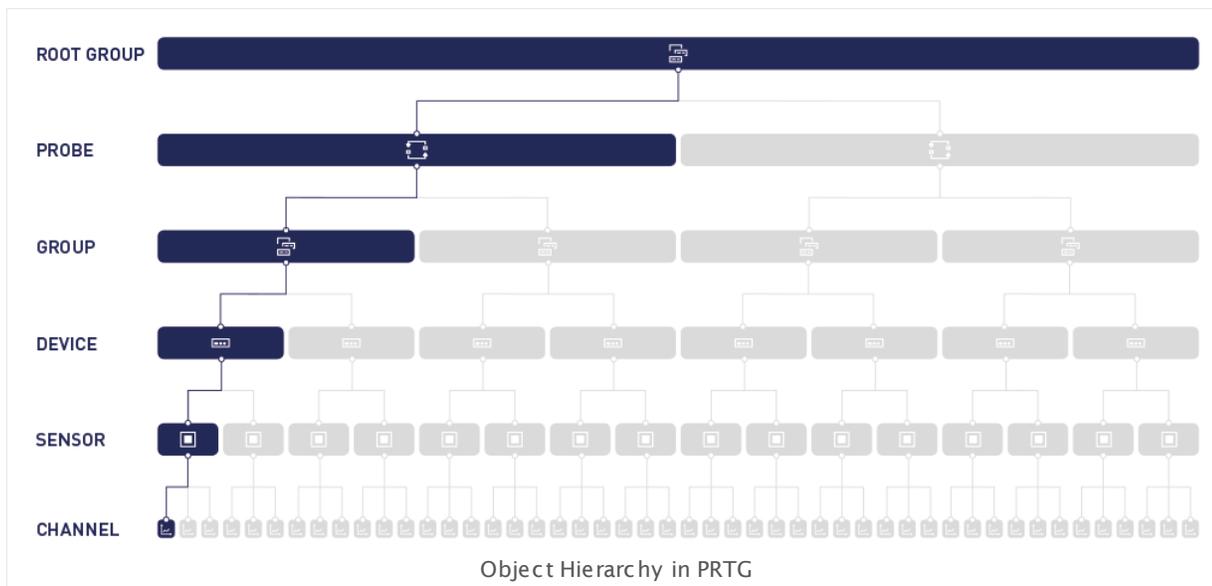
- <https://www.paessler.com/support/videos/prtg-advanced/cluster-animation>

Video Tutorial: How to set up a PRTG cluster

- <https://www.paessler.com/support/videos/prtg-advanced/how-to-set-up-a-cluster>

5.3 Object Hierarchy

All objects in a PRTG monitoring configuration are arranged in a tree-like hierarchy to create an easy-to-navigate list and to give the user the possibility to arrange them in groups that monitor similar devices, services, or particular locations. This hierarchical order is also used to define common settings for larger groups of objects, for example, settings of the **Root** group apply by default to all other objects underneath (see section [Inheritance of Settings](#)¹³⁷).



The figure shows the object hierarchy in PRTG:

- **Root** group contains all objects in your setup; all probes are directly under the root node.
- A **Probe** contains one or several groups.
- A **Group** contains one or several devices.
- A **Device** represents a physical or virtual component in your network that is reachable via an IP address. Several sensors are attached to one device.
- A **Sensor** monitors one single aspect of a device and has at least one channel.
- A **Channel** tracks one specific data stream and displays it as part of a sensor.

Root Group

The **Root** group is the topmost instance in PRTG. It contains all other objects in your setup. Using the [inheritance](#)¹³⁷ mechanism, we recommend that you [adjust the default settings for the Root group](#)³³¹. This will make configuration easier later on, because all other objects then inherit these standard settings by default. Thus, you will not have to set up the same configuration for each object anew.

Probe

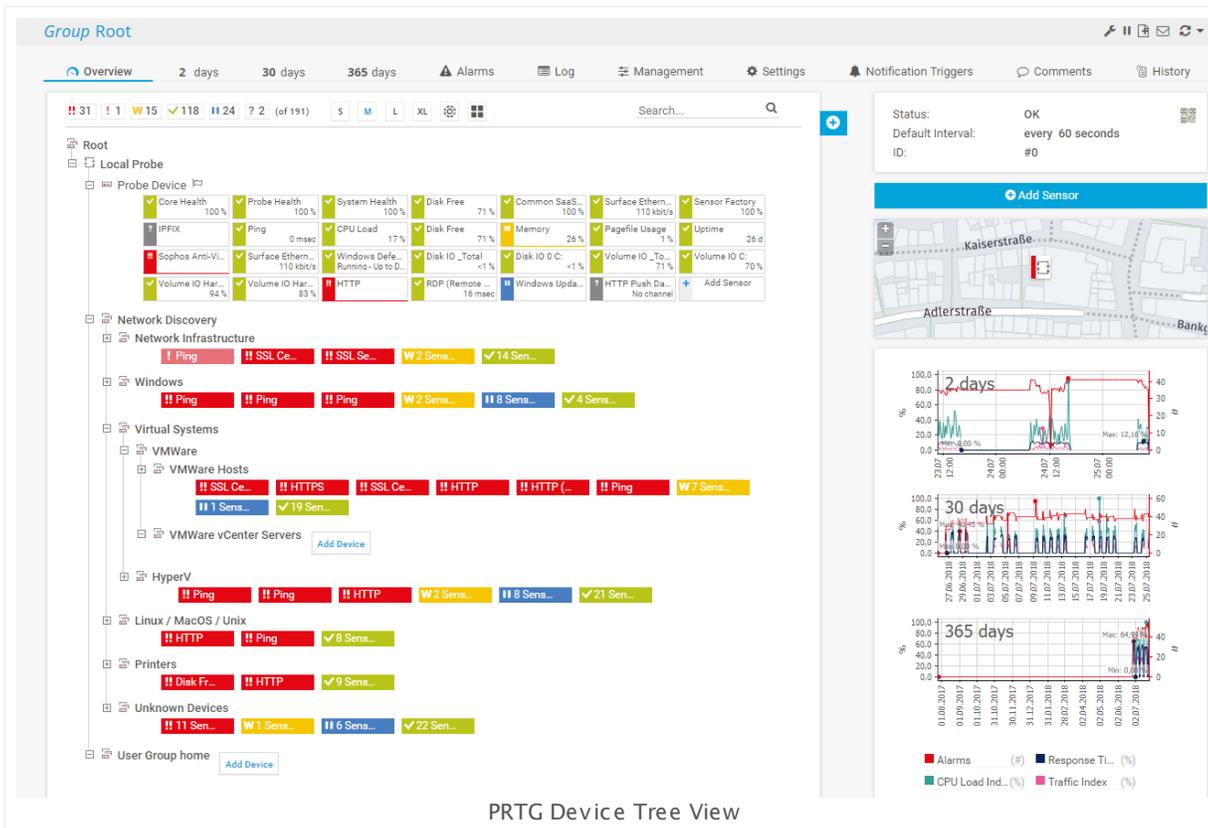
Each group (except the **Root** group) is part of a **Probe**. This is the platform where the monitoring takes place. All objects configured below a probe will be monitored via that probe. Every PRTG on premises core server installation automatically installs a **Local Probe** service, every PRTG hosted by Paessler instance comes with a **Hosted Probe**.

You can add additional probes and remote probes to your configuration to include remote devices from outside your network into the monitoring (see section [Multiple Probes and Remote Probes](#)). In a PRTG on premises cluster, there is an additional **Cluster Probe** running on all nodes. Devices on the cluster probe are monitored by all nodes of the cluster, so data from a different perspective is available and monitoring for these devices will always continue, even if one of the nodes fails.

Group

On each probe, there are one or more **Groups**, which serve merely structural purposes. Use groups to arrange similar objects so that they inherit the same settings. To a group, you add devices. You can arrange your devices in different nested groups to reflect the structure of your network.

Find below a sample configuration: A device tree with local probe, several groups, devices and their sensors.



PRTG Device Tree View

Device

You can add **Devices** that you want to monitor to each probe or group. Each device in your PRTG configuration represents a real hardware or virtual device in your network. These can be, for example:

- Web or file server
- Client computer (Windows, Linux, or Mac OS)
- Router or network switch
- Almost every device in your network that has its own IP address

 Sometimes you may want to add the same device in PRTG several times to receive a better overview when using a large number of sensors for very detailed monitoring, or to use different device settings for different groups of sensors. In PRTG you can simply add multiple devices with the same IP address or DNS name. The sensors on all of these PRTG devices will then query the same real hardware device in your network.

PRTG additionally adds a so called **Probe Device** to the local probe. This is an internal system device. It has access to the computer where the probe is running and monitors its health parameters with several sensors running on it.

To get a better and more detailed picture about your devices, PRTG automatically analyzes the devices that you add and recommends appropriate [sensor types](#)^[429] on the [device overview tab](#)^[198]. In the **Recommended Sensors** table, click the **Add These Sensors** button in the corresponding table row to create recommended sensor types with one click.

 You can turn off the sensor recommendation in [System Administration—Monitoring](#)^[339].

Sensor

On each device you can create a number of **Sensors**. Every sensor monitors one single aspect of a device. This can be, for example:

- One network service like SMTP, FTP, HTTP, etc.
- One network switch port's traffic
- CPU load of a device
- Memory load of a device
- Traffic on one network card
- One NetFlow device
- System health of a device
- Other content (for example, of databases, mails, HTTP, XML, files, etc.)
- etc.

 For more information, see this video tutorial: [What is a sensor?](#)

Channel

Every sensor has a number of **Channels** through which it receives the different data streams. The available channels depend on the type of sensor. One sensor channel can contain, for example:

- **Downtime** and **uptime** of a device
- **Traffic in** of a bandwidth device (for example, a router)
- **Traffic out** of a bandwidth device (for example, a router)
- **Traffic sum** of a bandwidth device (for example, a router)
- **WWW traffic** of a NetFlow device
- **Mail traffic** of a NetFlow device
- **Other traffic** of a NetFlow device
- **CPU load** of a device
- **Loading time** of a web page
- **Download bandwidth** of a web page
- **Time to first byte** of a web page
- **Response time** of a Ping request to a device
- **Response time** of a Remote Desktop service
- etc.

More

Video Tutorial: What is a sensor?

- <https://www.paessler.com/support/videos/prtg-basics/what-is-a-sensor>

5.4 Inheritance of Settings

The [hierarchical tree](#)^[133] does not only help organize the devices and keep everything neat and tidy. There is also an important aspect involved that we call **inheritance**. To ensure administration is quick and easy—especially for large monitoring setups—certain settings are inherited from the higher level. For example, you can change the monitoring interval for all sensors by editing the interval setting of the topmost **Root** group (unless no other setting is defined below).

Settings are Inherited to Child Objects

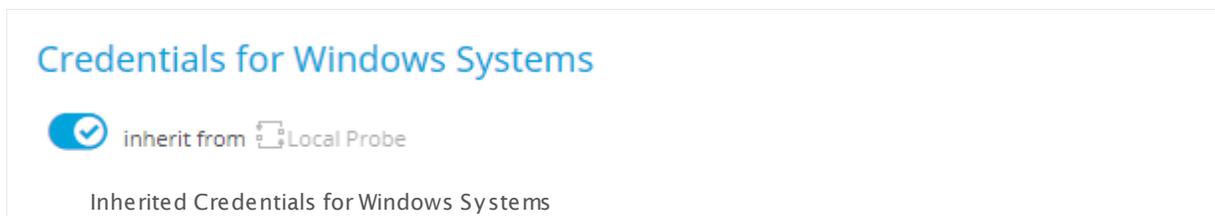
You can override this inheritance on any level of the hierarchy by setting a different value for a specific probe, group, device, or sensor. All objects below will inherit these new settings; object settings from levels above will not be affected.

Settings that are inherited among all objects include:

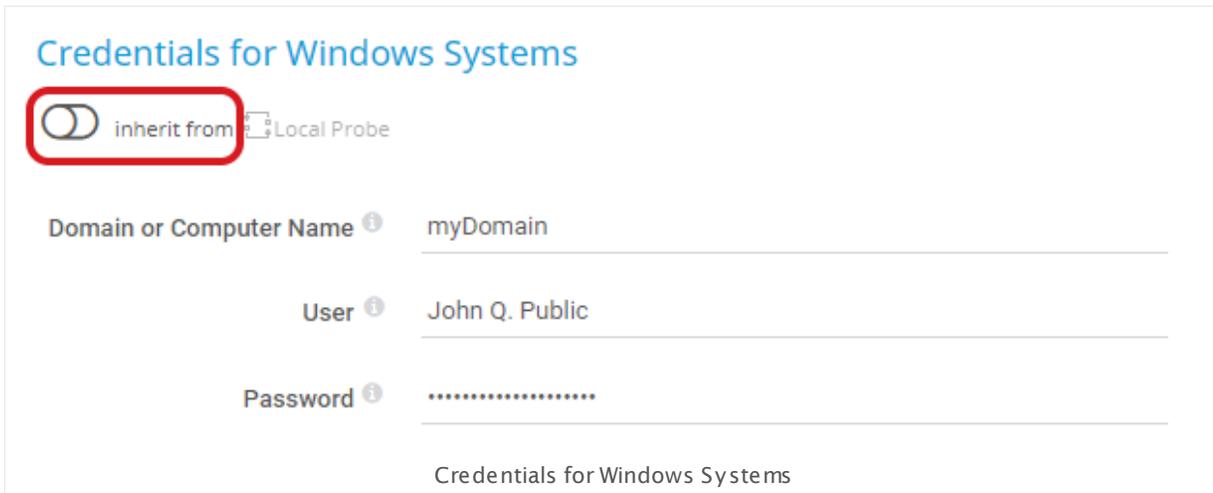
- Monitoring interval
- Notification triggers
- Authentication settings for several systems
- Compatibility settings (for certain types of sensors)
- Channel and unit configuration
- [User access rights](#)^[158]
- [Tags](#)^[139]
- Paused status: If an object is paused by the user, or a schedule, all sensors on it are paused as well

There is one exception for devices and sensors: the **IP address** or **DNS name** of a device and compatibility settings are always inherited by sensors and cannot be changed on sensor level.

The screenshot below shows the Windows systems credentials settings inherited from the parent.



Click  next to **inherit from [parent object]** to override the parent's settings and enter new settings for this object and all objects underneath in the hierarchy.



Credentials for Windows Systems

inherit from Local Probe

Domain or Computer Name ⓘ

User ⓘ

Password ⓘ

Credentials for Windows Systems

⚠ Click **Save** for your settings to take effect. Clicking after entering your settings inherits the parent settings again and your settings will not take effect.

Default Values Set in Root Group

For all settings (except passwords), PRTG already includes a set of default values so you can get started with the software immediately. For example, the following settings will be inherited by all sensors from the **Root** group:

- Default monitoring interval of one minute
- SNMP version 1 with community string set to **public** (default values for most devices)
- Dependency type **Use parent**
- etc.

You may need to change some of the default entries as you become used to the interface. However, these settings will initially suffice for most situations.

Before sensor setup, please review the **Root** group settings and set the default values to suit your setup. This should include the credentials for the types of systems in your network that you want to monitor (Windows, Linux, virtual servers, etc.).

📖 See section [Root Group Settings](#)^[331] for more details.

Inheritance of Notification Triggers

If you add notification triggers at probe, group, or device level, these will also be inherited to all sensors underneath, unless you break the inheritance manually.

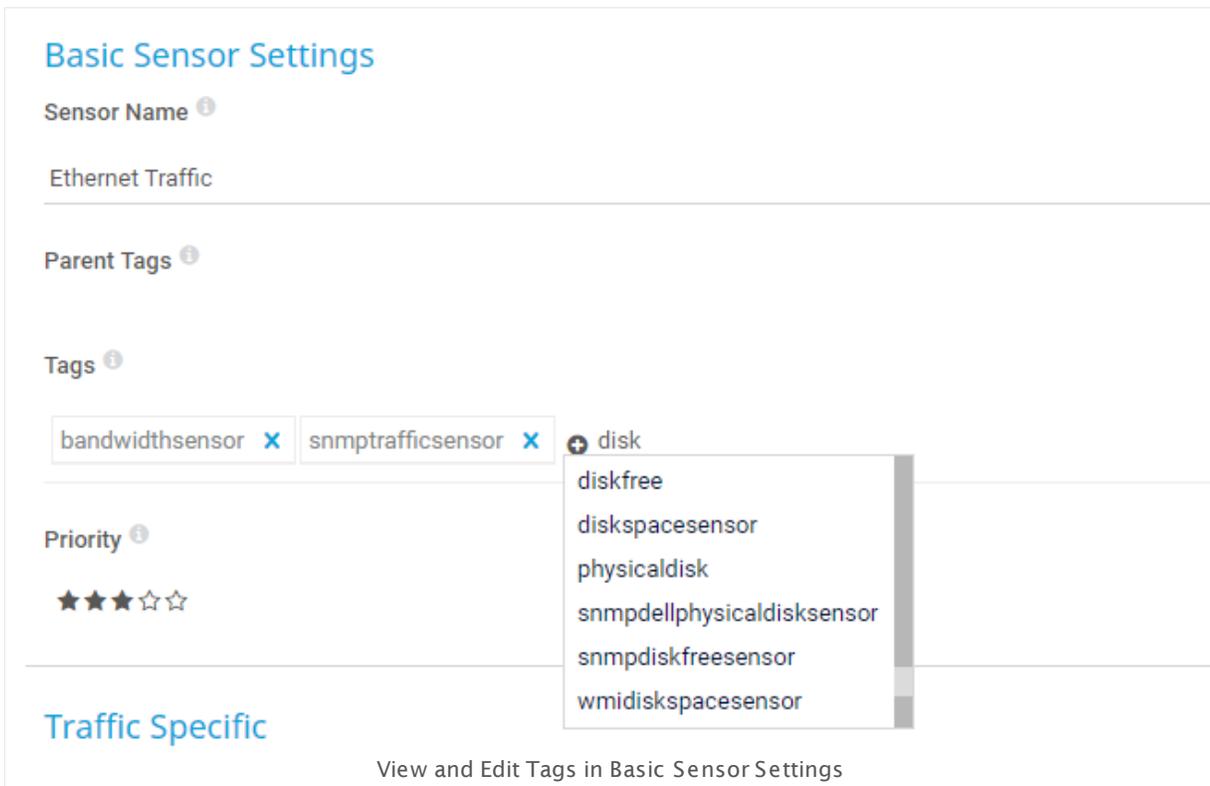
📖 See section [Sensor Notification Triggers Settings](#)^[3170] for details.

5.5 Tags

For every object in your PRTG setup, you cannot only name objects, you can also define tags in the [object settings](#)^[217] to additionally mark an object as a member of certain categories. Although some tags are automatically predefined when [adding objects](#)^[301], you are completely free in which tags you want to add. For example, you can mark all of the bandwidth sensors that are especially important for you with the tag **bandwidth_important**.

Later on, you can view lists of objects with certain tags (helpful for [multi-edit](#)^[3197] of settings), or select sensors via tags when creating [reports](#)^[3252]. A smart arrangement of tags can be a huge time saver. The keys enter, space, or comma confirm a tag.

- i** You can also change tags for several objects simultaneously using the [multi-edit](#)^[3197] function.
- i** It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).



Basic Sensor Settings

Sensor Name ⓘ
Ethernet Traffic

Parent Tags ⓘ

Tags ⓘ

bandwidthsensor × snmptrafficsensor ×

disk
diskfree
diskspacesensor
physicaldisk
snmpdellphysicaldisksensor
snmpdiskfreesensor
wmidiskspacesensor

Priority ⓘ
★★★★☆☆

Traffic Specific

View and Edit Tags in Basic Sensor Settings

Tags are Inherited

The tags in the settings of an object are automatically **inherited** by all other objects underneath in the **Object Hierarchy**. You can view inherited tags in section **Parent Tags** in the settings of a **sensor**, **device**, or **group**. So, for example, a device with the tag **myExampleTag** automatically passes on this tag to all sensors that you add to it. These sensors appear in lists whenever you search for **myExampleTag**. This is useful, for example, when you include sensors by tag in **reports** settings, because you do not have to tag every single sensor manually.

 Inheritance for tags cannot be disabled.

Filtering with Tags

You can use tags to filter **table lists** for specific objects, or to add sensors to **Libraries** and **Reports**. For example, you can restrict the **sensors overview page** to the sensors that have the tag **bandwidth_important**. You can also use more than one tag to filter for monitoring objects like sensors.

When filtering with tags, you can also use plus (+) and minus (-) signs in front of the tags to include or exclude them:

- Tags with + must exist for an object to be shown
- Tags with - must **not** exist for an object to be shown
- At least one tag of the tags without either a + or - must exist on an object

The filter shows an object only if all three conditions are true. The order of the tags in a tag field does not matter.

For example, if you enter **-windows** into a tag field, all sensors/devices that do not have "windows" as tag are shown. With **+windows** or **windows** you filter for objects that are tagged with "windows".

You can use more than one logical operator in a tag field: For example, if you enter **+netflow - bandwidth_important** into a tag field, the corresponding list, library, or report includes all sensors that are tagged with "netflow" but not with the tag "bandwidth_important". If you enter **netflow bandwidth_important**, a sensor has to be tagged with "netflow" or "bandwidth_sensor" or both to be affected.

Tag Display Limits

For performance reasons, PRTG has a display limit of 1000 tags when filtering **By Tag** under **Sensors** in the **PRTG main menu**. If you have more than 1000 tags, no tags are shown here. You can still use tags in this case, for example, for filtering and searching.

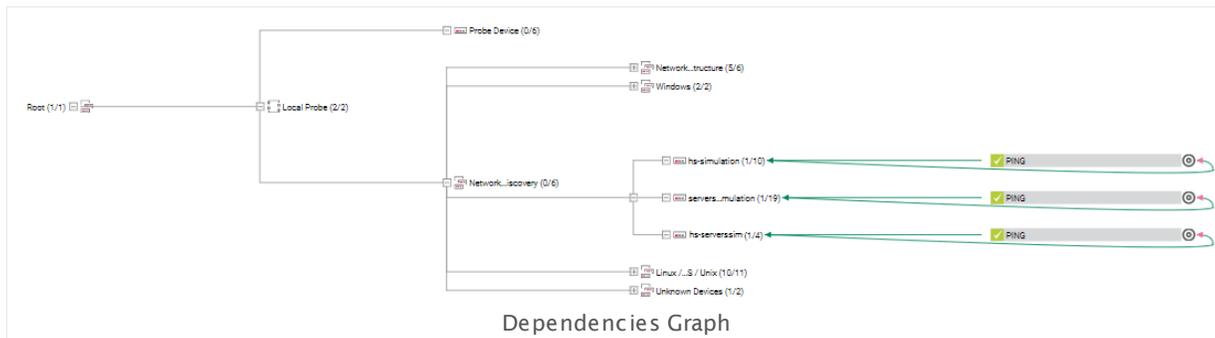
5.6 Dependencies

You can use dependencies to make PRTG pause sensor monitoring based on the [status](#)^[195] of another (master) sensor to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as a specific sensor is in **Down** status or in **Paused** status caused by another dependency. This means, for example, that you can stop monitoring remote network services when the corresponding firewall is down due to connection problems.

When using the [auto-discovery](#)^[282] function, the [Ping Sensor](#)^[1529] on a device is by default set as the **master** object for this device. This means that monitoring for the entire device is paused if the Ping sensor is in **Down** status or in **Paused** status caused by another dependency. Usually, it makes little sense to monitor any other parameters while the **Ping** sensor indicates that the device can't even be reached.

i You do not trigger a status change by dependency if you manually pause a master object or if you pause it by [schedule](#)^[142]. See also this Knowledge Base article [Why will dependent objects not go into paused status automatically when I pause the master object?](#)

To view the list of dependencies, choose **Devices | Dependencies** and the corresponding dependencies path from the [main menu](#)^[265]. From there you can also access the [Dependencies Graph](#)^[3209] that visualizes all dependencies within your network.



+ For more information about the dependency settings, see the [settings of the object](#)^[217] you want to set a dependency for, section [Schedules, Dependencies, and Maintenance Window](#)^[422] respectively.

5.7 Scheduling

With the help of schedules you can [pause](#)^[245] the monitoring of certain objects automatically for a certain time, for example, on Sundays between 4 and 8 a.m. A paused sensor will not collect monitoring data, will not change its status, and will not trigger any [notifications](#)^[143]. You can also pause monitoring for planned system maintenance time spans to avoid false alarms. You can apply different schedules to every object. Schedules are also used for reports and notifications.

i If you pause a master object by schedule or manually, you do not trigger a status change by [dependency](#)^[141]. See also this Knowledge Base article [Why will dependent objects not go into paused status automatically when I pause the master object?](#)

Schedules, Dependencies, and Maintenance Window

inherit from Root

Dependencies, schedules and maintenance windows always pause all sensors inside a group/device. This pausing is always inherited to all sub-objects and the inheritance can not be disabled. Below you can set additional schedules, maintenance windows or dependencies that will be used on top of any inherited setting.

Schedule ⓘ	None ▼
Maintenance Window ⓘ	None
Dependency Type ⓘ	Saturdays [GMT+0100]
	Sundays [GMT+0100]
	Weekdays [GMT+0100]
	Weekdays Eight-To-Eight (8:00 - 20:00) [GMT+0100]
	Weekdays Nights (17:00 - 9:00) [GMT+0100]
	Weekdays Nights (20:00 - 8:00) [GMT+0100]
	Weekdays Nine-To-Five (9:00 - 17:00) [GMT+0100]
	Weekends [GMT+0100]

Access Rights

inherit from Root

Available Default Schedules in Device Settings

Schedules are user account specific. To change the default pre-defined schedules or to add your own schedule, see [Account Settings—Schedules](#)^[338] section.

i If you use failover clustering with nodes in different timezones, scheduling applies at the local time of each node. For more information, see section [Failover Cluster Configuration—Before Getting Started](#)^[372].

5.8 Notifying

PRTG Network Monitor keeps the administrator or other responsible persons informed about the current status of the network. There are several methods how the administrator can stay up to date.

Notifications

This is the most powerful information tool. Whenever PRTG discovers downtime, an overloaded system, threshold breaches (for example, a disk runs full), or similar situations, it can send a notification. Notifications use various methods with which you can be notified (for example, [email](#)^[3317], [SMS](#)^[3311], [push messages](#)^[3319], and others). After creating notification templates in the system settings, you can select them on the notification triggers tab of probes, groups, devices, and sensors, as well as on the root group.

 See [Notifications](#)^[3216] section for more details and [Setting Up Notifications Based on Sensor Limit: Example](#)^[3219] for a step-by-step guide.

Limits

In a [sensor channel's settings](#)^[3160], you can set limits to change the status of the sensor when certain limits are breached. This way, you can set, for example, a traffic sensor (typically never in an error status) to **Down** status whenever bandwidth values are measured that you consider critical. This sensor will then show up in the alarms list.

Alarms

The alarms list shows all sensors that are currently in a **Down**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. This is useful for keeping track of all irregularities in your network. In the table list, you can re-sort the items by clicking on the column's header items. See [Alarms](#)^[219] section for more details.

Logs

In the logs list, the logfile with all monitoring events is shown. In a typical setup, a huge amount of log data is produced. As the activity of every single object is minuted, you can use this data to check exactly if your setup works as expected. See [Logs](#)^[228] section for more information.

Tickets

The tickets list shows items with important system information or action steps for the administrator to take. You should view every ticket and take appropriate actions. By default, an email is sent to the administrator for every new ticket that is created by the system or another user. If a ticket is assigned to a specific user, this user will get an email by default. See [Tickets](#)^[230] section for more information.

5.8.1 Alerts

Alerting is a helpful and important part of monitoring that informs you when there are issues, when values exceed thresholds or a sensor status has changed, for example. PRTG offers many ways to alert you about your monitoring data like internal sensor alerts, limits, and lookups. You can also create custom alerts and define trigger notifications as extensions to alerts. If a sensor does not have pre-configured limits, you can also configure them accordingly so that you are notified when something is wrong.

Internal Sensor Alerts

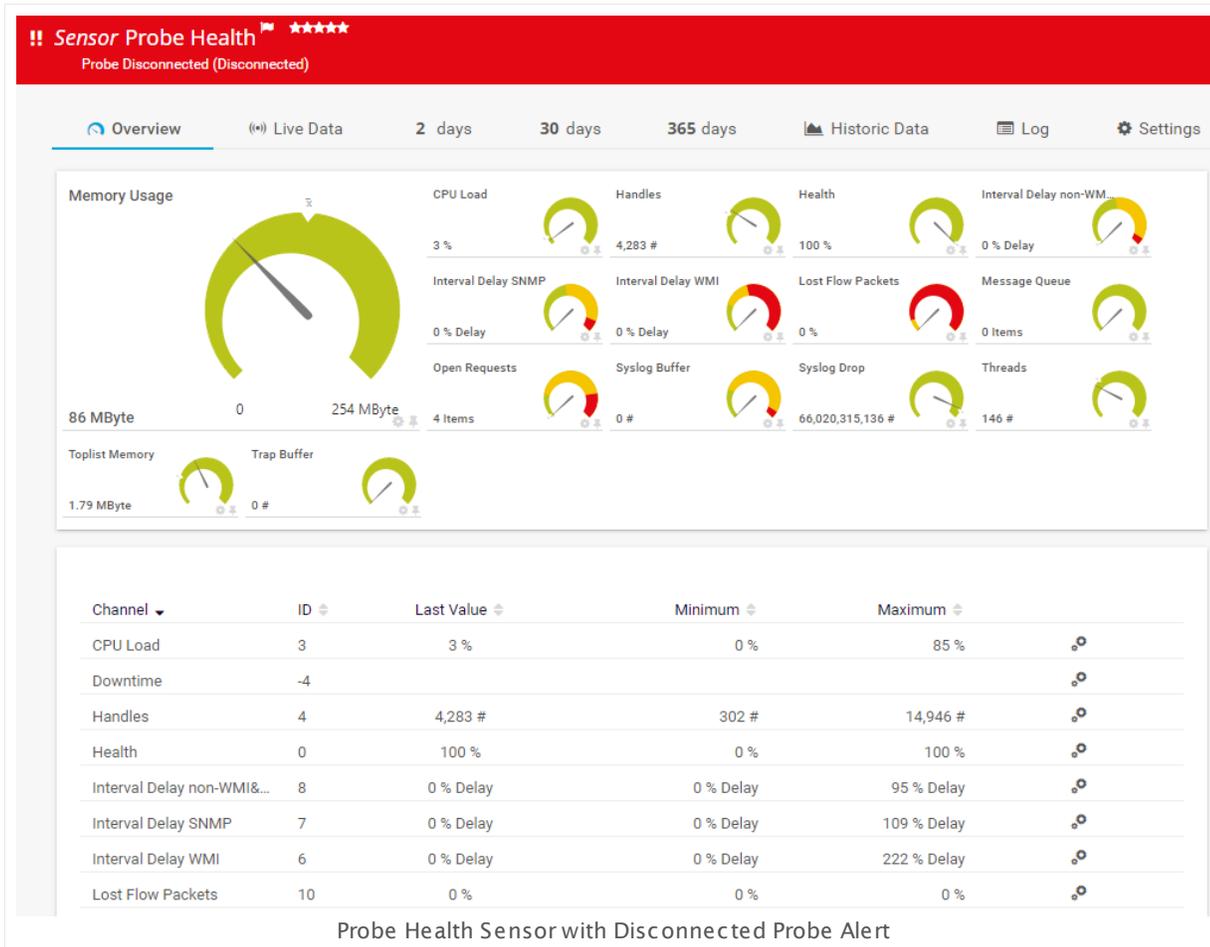
Some sensor types display internal alerts when there are errors. These default alerts range from disconnected probes to socket or timeout errors. For example, the HTTP sensors show pre-configured internal alerts according to certain HTTP status codes.

There are also sensor types that let you modify the internal sensor alerts. To see if you can modify an alert, check the sensor's settings for customizable options.

 See [Which HTTP status code leads to which HTTP sensor status?](#) for more information.

 See [What does error code PExxx mean?](#) for more information on error codes.

Here is an example of a sensor that is in **Down status**  because of an internal sensor alert.



Standard Limits for Channels

Another type of alerts are alerts due to limits. These alerts are triggered when the measured value of a sensor is below or above a configured threshold limit. These limits change the sensor's status when they are breached. For example, you can set an SNMP CPU Load sensor to **Warning** status whenever it measures values that you consider critical. This sensor then shows up in the [alarms](#) list.

- i This type of alert is only displayed when the value breaches the configured limits. If the value is normal again in the next sensor scan, the sensor returns to the **Up** status.
 - To review or modify threshold limits for single sensors, open the [sensor's channel settings](#) via the gear icon in the respective channel gauge or in the channels table.
 - **Enable alerting based on limits** and specify your desired limits in the correct fields.
 - You can also optionally add messages that appear in the sensor message on the **Overview** tab or leave these fields empty to display the default message.
- i This limit only applies to the respective channel.

Part 5: Understanding Basic Concepts | 8 Notifying
1 Alerts

Edit Channel ✕

CPU Load (Tables Only) (ID 5) ▼

Edit Channel "CPU Load"

Name ⓘ
CPU Load

ID ⓘ
5

Limits ⓘ
 Disable limits
 Enable alerting based on limits

Upper Error Limit (%) ⓘ
80

Upper Warning Limit (%) ⓘ
60

Lower Warning Limit (%) ⓘ

Lower Error Limit (%) ⓘ

Error Limit Message ⓘ
CPU usage is high!

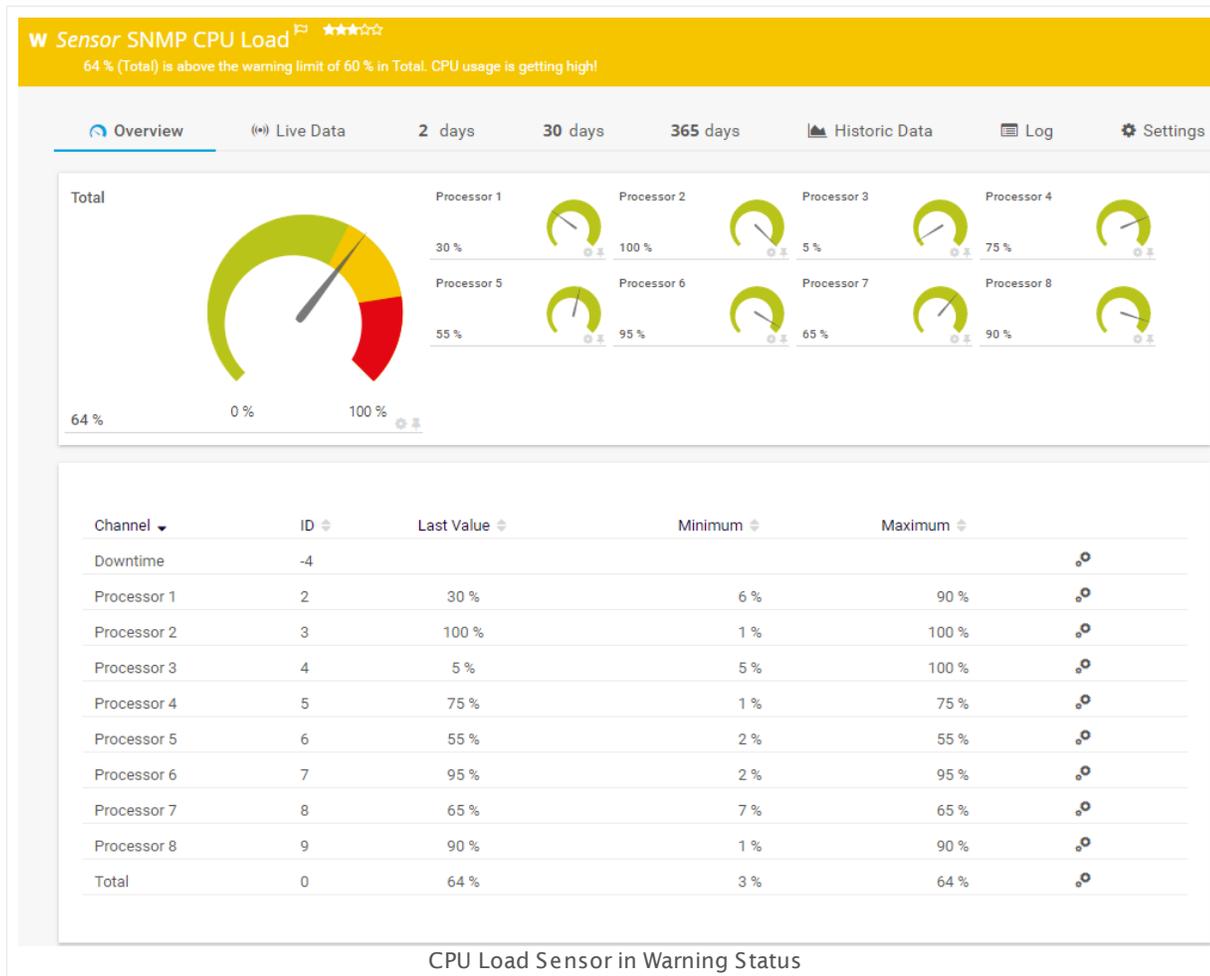
Warning Limit Message ⓘ
CPU usage is getting high!

Graph Rendering ⓘ
 Show in Graphs
 Hide from Graphs

Setting Limits for Sensor Channels

📺 For more information on setting limits, see this video on our website: [How to Set Channel Limits](#)

With the above configuration, the sensor turns to a **Warning** status (the gauge needle points to the yellow area in the example below) if the channel values exceed the upper warning limit of 60 percent and the **Warning Limit Message** is displayed in the sensor status. If the channel value exceeds the upper error limit of 80, the sensor will turn to a **Down** status (the gauge needle will point to the red area) and the **Error Limit Message** will be displayed.



You can use [Multi-Edit](#) if you want to apply the same limits for sensors of the same type in a batch operation.

- To see all sensors of this type at a glance, just filter for it: From the PRTG main menu bar, choose **Sensors | By Type | SNMP CPU Load**.
- Mark the check boxes of the sensors you want to edit.
- Click the wrench symbol in the menu.
- Open the **Channel Settings** tab.
- Select the channel you want to add a limit for; in this example we use the channel **Total**, which is common to all selected sensors.
- Then **Enable alerting based on limits** and enter the number in the correct field as described above.

When you are done, **Save** these settings—the new limit is then applied to all selected channels from all selected sensors.

Multi-edit is only available for channels that are common to all selected sensors.

Part 5: Understanding Basic Concepts | 8 Notifying 1 Alerts

Editing 3 Objects
✕

Edit Channel

- Limits** ⓘ
 - Disable limits
 - Enable alerting based on limits
- Upper Error Limit (%)** ⓘ

- Upper Warning Limit (%)** ⓘ

- Lower Warning Limit (%)** ⓘ

20
- Lower Error Limit (%)** ⓘ

- Error Limit Message** ⓘ

- Warning Limit Message** ⓘ

- Graph Rendering** ⓘ
 - Show in Graphs
 - Hide from Graphs
- Table Rendering** ⓘ
 - Show in Tables
 - Hide from Tables
- Line Color** ⓘ
 - Automatic
 - Manual
- Line Width** ⓘ

Cancel OK

Setting Channel Limits with Multi-Edit

ⓘ Some sensors have pre-defined limits in the sensor settings, for example the [SNMP Linux Disk Free Sensor](#)^[2251]. Refer to the sensor's settings to adjust the limits (or behavior) for these sensors.

Absolute and Delta Values in Limits

- i** The value that needs to be configured in the limits depends on the type of data that the sensor's channel delivers.

For channels that measure absolute values (for CPU load and memory usage, for example) limits will also be set using absolute values like in the example above.

You can also set limits for channels that measure delta (x.xx/sec) values. Let's say you have an [SNMP Traffic Sensor](#) and want to receive an alert when it reports errors. In this case, you need take into account that this is a delta measurement. In this example, you could set the following limits for the channel **Errors in** with a standard scanning interval (60 seconds).

- Set the sensor to **Warning** status when **1** error occurs
- Set the sensor to **Down** status when **30** errors occur

This example shows how to configure the limits for delta channels.

Part 5: Understanding Basic Concepts | 8 Notifying
1 Alerts

Edit Channel ✕

Errors in (ID 10) ▼

Edit Channel "Errors in"

Name ⓘ
Errors in

ID ⓘ
10

Limits ⓘ

Disable limits
 Enable alerting based on limits

Upper Error Limit (#/s) ⓘ
0.5

Upper Warning Limit (#/s) ⓘ
0.1

Lower Warning Limit (#/s) ⓘ

Lower Error Limit (#/s) ⓘ

Error Limit Message ⓘ

Warning Limit Message ⓘ

Graph Rendering ⓘ

Show in Graphs
 Hide from Graphs

Table Rendering ⓘ

Show in Tables

Setting Channel Limits with Delta Values

Because this channel uses per second (delta) measurements, a single error that occurs over a standard 60-second scanning interval is reported as 0.016 # per second. So the warning limit for one single RX error within an interval is 0.1 (errors/sec). To get an alert when there are 30 errors within a scanning interval, the limit needs to be 0.5 (errors/sec).

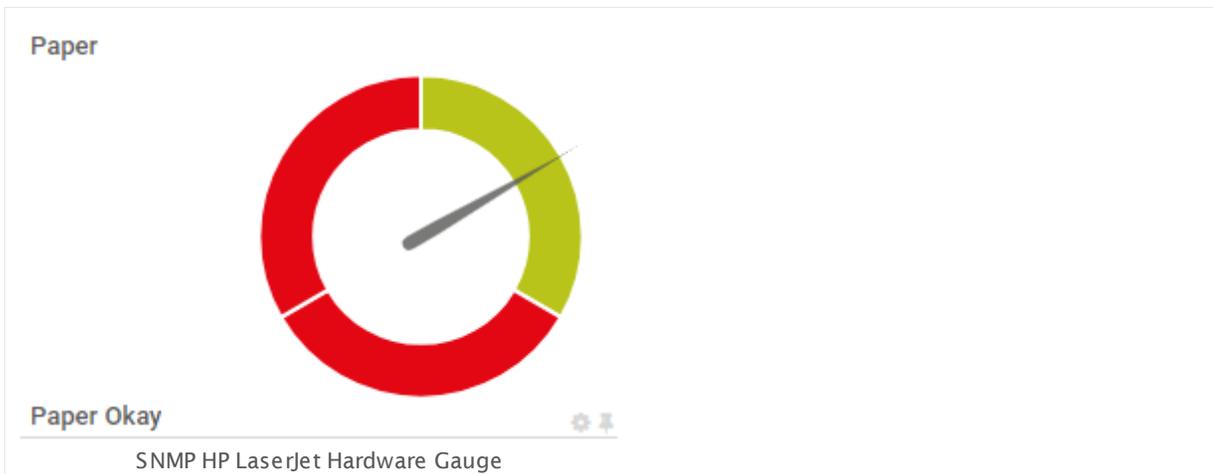
! If no new errors occur in the next scanning interval, the sensor will turn back to the **Up** status. To ensure that you do not miss any notifications for this sensor, set a notification trigger with **0** seconds. For more information, see [Notification Triggers as Extensions to Alerts](#)¹⁵⁵ below.

Standard Lookups for Channels

PRTG also uses lookups for some sensor types. In general, lookups make data more human friendly because they map status values as returned by a device (usually integers) to more informative expressions in words that show you the status of a monitored device as a clear message.

Additionally, lookups can also define the sensor status that will be shown in correlation with certain status codes, just like sensor channel limits can define a sensor status, too. For example, PRTG can show a sensor in a gray **Inactive** status with channel values, provided by lookups, like **Inactive** instead of a numerical value like **-1**.

i The various states displayed in gauges always follow the clockwise order **Up** (green) < **Warning** (yellow) < **Down** (red) < **Unknown** (Gray / Black).



Modifying a Standard Lookup: Example

You can also modify standard lookups to include new definitions according to your monitoring needs. The following code illustrates the lookup definition for the paper status of the [SNMP HP LaserJet Hardware](#)²¹⁰⁸ sensor:

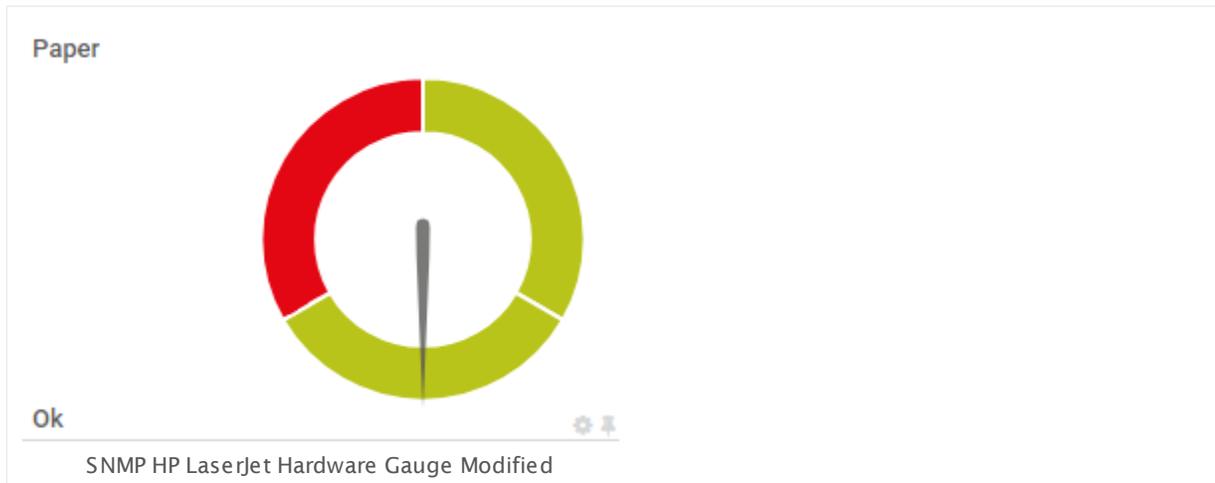
Part 5: Understanding Basic Concepts | 8 Notifying 1 Alerts

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.paperstatus" desiredValue="0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation=
"PaeValueLookup.xsd">
  <Lookups>
    <SingleInt state="Ok" value="0">
      Paper Okay
    </SingleInt>
    <SingleInt state="Error" value="1">
      Out of Paper or No Cassette Loaded
    </SingleInt>
    <SingleInt state="Error" value="2">
      Manual Paper Feed Required
    </SingleInt>
  </Lookups>
</ValueLookup>
```

Imagine you do not want to be alerted in case the printer is out of paper. You basically have to do the following:

1. Copy the file `oid.paessler.hplaserjet.paperstatus.ovl` to the `\lookups\custom` subfolder of the [PRTG program directory](#) (ensure you do not change the file name!).
2. Open this file with an editor.
3. Replace the first `SingleInt` state "Error" with "Ok".
4. Optionally replace the message "Out of Paper or No Cassette Loaded" to "Ok".
5. Save the file.
6. [Reload](#) the custom lookup folder in PRTG.

The channel gauge now displays the new state and the new message.oid



For more information on how lookups are defined, see section [Define Lookups](#).

Creating a New Lookup

It is also possible to create new lookups to use with any custom or standard sensor that supports lookups. If you want to create a new lookup with the [example](#) above, you basically follow the same procedure except you save the lookup file in the `\lookups\custom` subfolder with a new name, for example `oid.paessler.hplaserjet.mynewpaperstatus.ovl`. Select the newly created lookup file in the sensor's channel settings.

Part 5: Understanding Basic Concepts | 8 Notifying 1 Alerts

Edit Channel
✕

Toner (ID 3)
▼

Edit Channel "Toner"

Name
Toner

Unit ⓘ

Scaling Multiplication ⓘ

Scaling Division ⓘ

ID ⓘ
2

Value Lookups and Limits ⓘ

Enable alerting based on value lookups
 Enable alerting based on limits

Value Lookup ⓘ
oid.paessler.hplaserjet.mynewtonerstatus ▼

Graph Rendering ⓘ

Show in Graphs
 Hide from Graphs

Table Rendering ⓘ

Show in Tables
 Hide from Tables

Line Color ⓘ

Automatic
 Manual

Apply
Ok
Cancel

Selecting a Newly Created Lookup

Custom String Lookups

You can also set up custom string lookups, which can exclusively be used with the [SNMP Custom String Lookup Sensor](#)^[1982]. This is useful if you are using an OID that returns a known string value stating possible states or values. To inform PRTG of the possible statuses or values, you have to create a new lookup file defining them.

See the Knowledge Base article [Monitor and "Lookup" a SNMP String value](#) for more information.

Notification Triggers as Extensions to Alerts

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. Which trigger types are available depends on the kind of object you edit. You can define triggers that are activated by an 'on change' event. Some sensors offer the option to send such a trigger whenever sensor values have changed.

Create Notification Triggers to Alert You When a Value Changes

Before you set up a change trigger, make sure that the **Trigger 'change' notification** setting is enabled in the sensor's settings, otherwise the notification will never be sent.

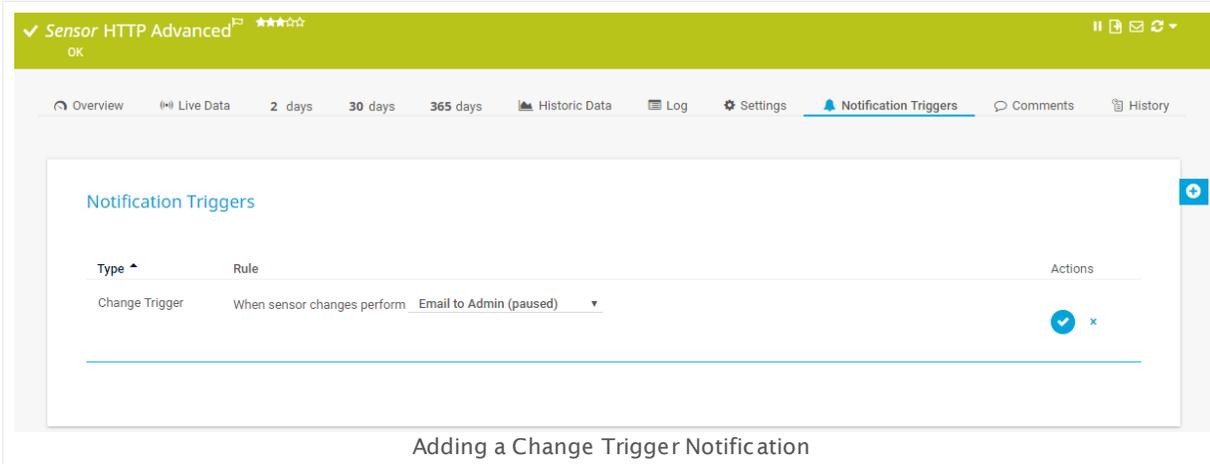
Advanced Sensor Data

Protocol Version ⓘ	<input type="radio"/> HTTP 1.0 <input checked="" type="radio"/> HTTP 1.1
User Agent ⓘ	<input checked="" type="radio"/> Use PRTG's default string <input type="radio"/> Use a custom string
HTTP Headers ⓘ	<input checked="" type="radio"/> Do not use custom HTTP headers <input type="radio"/> Use custom HTTP headers
Content Changes ⓘ	<input type="radio"/> Ignore changes <input checked="" type="radio"/> Trigger 'change' notification
Require Keyword ⓘ	<input checked="" type="radio"/> Do not check for keyword (default) <input type="radio"/> Set sensor to warning if keyword is missing <input type="radio"/> Set sensor to error if keyword is missing
Exclude Keyword ⓘ	<input checked="" type="radio"/> Do not check for keyword (default) <input type="radio"/> Set sensor to warning if keyword is found <input type="radio"/> Set sensor to error if keyword is found
Limit Download (kb) ⓘ	0
Result Handling ⓘ	<input checked="" type="radio"/> Discard HTML result <input type="radio"/> Store latest HTML result

Trigger 'Change' Notification Setting

Part 5: Understanding Basic Concepts | 8 Notifying 1 Alerts

Select the **Notification Triggers** tab to create a change trigger for this sensor. Hover over  and select **Add Change Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing trigger to change it. Every trigger will provoke one or more [notification\(s\)](#)  to be executed.



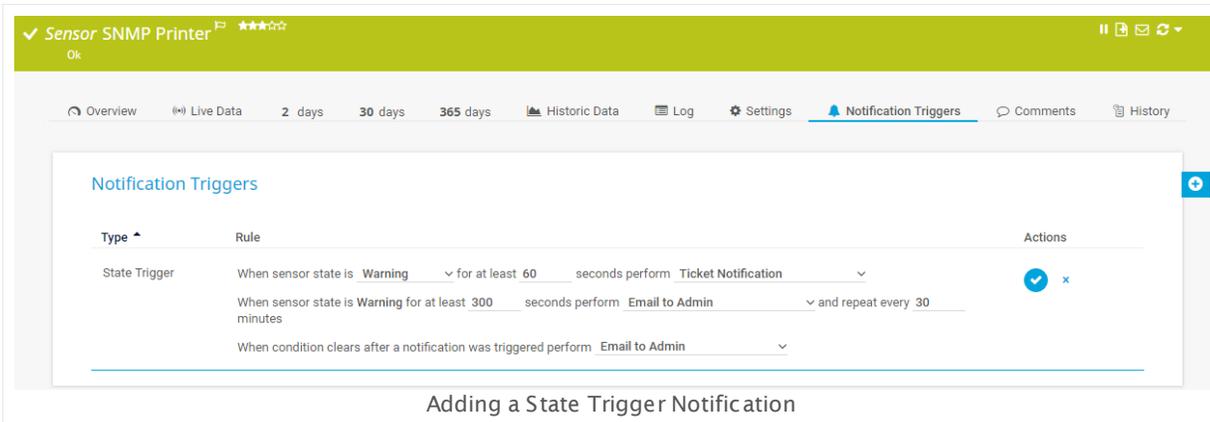
Adding a Change Trigger Notification

Save the trigger. You will now be notified when sensor values change.

 For more information on triggers, see section [Sensor Notification Triggers Settings](#) .

Create Triggers to Match Your Limits/Lookups (status-based)

After you have set up alerts using limits or lookups, you can complement them with state-based triggers. On the **Notification Triggers** tab, hover over  and select **Add State Trigger** from the menu to add a new trigger.



Adding a State Trigger Notification

Save the trigger. You will now be notified according to the notification settings.

 If you want to receive alerts for more than one status, you have to add a trigger for each status.

-  A sensor's status can change for other reasons such as [internal sensor alerts](#)¹⁴⁴. If you configure state-based triggers, you will be notified of these changes as well.

More

Knowledge Base: Monitor and "Lookup" a SNMP String value

- <https://kb.paessler.com/en/topic/71098>

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: What does error code PExxx mean?

- <https://kb.paessler.com/en/topic/32813>

Video Tutorial: How to Configure Lookups in PRTG Network Monitor

- <https://www.paessler.com/support/videos/prtg-advanced/prtg-lookups>

5.9 User Access Rights

Define which user can access what in your PRTG Network Monitor installation and manage all user rights with the access rights system of PRTG.

The default administrator can be the only user of a PRTG installation, but can also create a nearly unlimited number of other users. Individual users are organized in a nearly unlimited number of user groups. Each user group can separately have [access rights for each individual object](#)^[133] in your PRTG device tree (except for sensor channels). Objects can also [inherit](#)^[137] access rights according to the hierarchic structure of the device tree.

In addition, every user has specific rights: There are administrator users, read/write users, and read-only users. You can define these settings in [System Administration—User Accounts](#)^[3376]. Via these tools, you can create an access rights management that allows you to specify exactly what users will be able to see and edit and what they will not be able to access.

Account Control

Account Type ⓘ	<input type="radio"/> Read/write user <input checked="" type="radio"/> Read-only user
Acknowledge Alarms ⓘ	<input type="radio"/> User may acknowledge alarms <input checked="" type="radio"/> Deny the right to acknowledge alarms (default)
Password Changes ⓘ	<input type="radio"/> User may change the account's password <input checked="" type="radio"/> Deny the right to change the password (default)
Primary Group	PRTG Users Group ▼
Status ⓘ	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Last Login ⓘ	5/29/2017 5:19:07 PM

User Rights in User Account Settings

Individual user rights, in combination with the access rights of the group(s) they belong to, determine the access rights to certain objects in the device tree. This means that group membership specifically determines what a user is allowed to do and which objects the user will see when logged in.

The actual access rights for each object in the device tree can be defined in the object's settings. You can define different access rights for all sensors, devices, groups, or probes via the corresponding [Context Menus](#)^[247] or in the [Object Settings](#)^[217].

Access Rights Overview

The following classes of access rights for objects are available in hierarchical order as they can be given to user groups (lowest rights to highest rights):

- **None:** The object will not be displayed to the users of the group; no logs, no tickets, no alarms regarding this object will appear.
- **Read:** You can only see monitoring results and change your own password if allowed by your administrator.
- **Write:** You are allowed to review monitoring results and edit settings. In addition, you can add objects to and delete them from the device tree.
- **Full:** Review monitoring results, edit settings, and edit access rights. In addition, you can add objects to and delete them from the device tree.
- **Admin rights:** If a user group has administrator rights, all options are available, including creating users, creating user groups, and deleting objects from the device tree. Users in the administrator user group always have maximum access rights to all objects and will never have access restrictions.

i Access rights that are defined locally on an object, for example, on a device, override inherited rights. For a certain object, the highest directly defined access right applies for a user group. If there is no access right set directly on an object, the next higher object level will be checked for access rights. This process is repeated until defined access rights are found to be [inherited](#) or there is no higher object level.

Edit Rights for Sonicwall Firewall
✕

Edit Access Rights

Use this page to review and edit access right for an object.
[Help: User Account Settings](#)

Current Access Rights

AD-Testgroup	Full	Admin User
PRTG Administrators	Full	Admin User
PRTG Users Group	Write	Inherited from 1st group »
Test1	None	Inherited from Root »
Test2	None	Inherited from Root »
test3	None	Inherited from Root »
User GroupActiveDirectory	None	Inherited from Root »
UserGroup1250	None	Inherited from Root »

<< < 1 to 8 of 8 > >>

Access Rights

inherit from 1st group

Cancel Continue >

Different Access Rights Depending on User Groups

See the table below for which user rights apply when. Column headings show access rights of user groups for objects in the device tree; line headings show the type of user.

i Users are either members in PRTG user groups or in Active Directory Domain user groups. They cannot be members in both. We recommend that you use only one type of user group (either PRTG or Active Directory) to minimize your administration effort.

▪ PRTG User Group	▪ PRTG User Group	▪ PRTG User Group	▪ PRTG System Administrator
▪ Domain User Group	▪ Domain User Group	▪ Domain User Group	▪ Domain Administrator
READ ACCESS	READ/WRITE ACCESS	FULL ACCESS	

- **PRTG User Read Only** Read-only rights Read-only rights Read-only rights Admin rights
- **Domain User Read Only**
- **PRTG User Read/Write** Read-only rights Read/write rights Full access Admin rights
- **Domain User Read/Write**
- **Users in an administrator group** always have administrator access rights, no matter what access rights have been defined for an object.
- **Read-only users** just have reading permission, no matter what access rights their group has. Users who are members of an administrator group are an **exception**. Read-only users can change their own passwords in their [user account settings](#)³³⁷⁶, if the administrator has enabled them to do so.
- **Read/write users** in a group with full access to a given object have full access rights to this object only.
- If a user is in **more than one group**, access rights of the user group with the highest rights apply.
- Administrator rights can only be granted by membership in the **administrator group**.

 For more information about defining access rights, see the following sections:

- [System Administration—User Accounts](#)³³⁷⁶
- [System Administration—User Groups](#)³³⁸³

 For information about connecting PRTG to an existing Active Directory, see [Active Directory Integration](#)³⁶⁰³.

5.10 Data Reporting

With [Reports](#) ³²⁵² you can analyze and review monitoring data for specific time spans. There are several ways to create data reports in PRTG for your individual needs.

View Historic Data

To get a report for a single sensor, there is a function included to review historic data in PRTG. It allows you to generate reports and charts for a single sensor's data. See the [Historic Data Reports](#) ²⁰⁴ section for more information.

Generate Reports

You can use the sophisticated reports machine included in PRTG to create comprehensive and detailed reports for all monitoring data. See the [Reports](#) ³²⁵² section for more information.

Export Data Using the API

You can also export all monitoring raw data to XML or CSV files and generate your own reports using any third-party software. See the [Application Programming Interface \(API\) Definition](#) ³⁶⁰⁰ section for more information.

Make Data Available

You can make monitoring data available to other persons using a special user with read-only rights (see the [User Access Rights](#) ¹⁵⁸ section), or you can create public or semi-public HTML pages with monitoring data using the Maps feature. See the [Maps](#) ³²⁷⁰ section for more information.

Bill Customers

You can also create custom billing reports based on PRTG's monitoring data, using the open source **Billing Tool** for PRTG.



For details and download, see the Paessler website: [Billing Tool](#)

More

- [Data Storage](#) ³⁷³⁴

Paessler Website: Billing Tool

- <https://www.paessler.com/tools/billingtool>

5.11 IPv6

PRTG supports the IPv6 protocol for most sensor types. You can choose whether you want PRTG to query data from your network devices via an IPv4 or IPv6 connection. Indicate your preference in the [Device Settings](#)^[402] of each device. The sensors you add to the device will use the protocol you have indicated.

In the **Outgoing IP Settings** of the [PRTG Administration Tool](#)^[3592], you can additionally choose which IPv6 address will be used for outgoing monitoring requests. The the same option is also available for IPv4.

-  Not all sensor types are IPv6 compatible. You can see which sensors support IPv6 in the [Add Sensor](#)^[328] dialog. Incompatible sensors are not selectable on IPv6 devices.
-  The [Cloud HTTP Sensor](#)^[619] and the [Cloud Ping Sensor](#)^[629] do not support IPv6 although you can add them to IPv6 devices. You will receive an error message if you do so.

Part 6

Ajax Web Interface—Basic Procedures

6 Ajax Web Interface—Basic Procedures

The PRTG web interface is the feature complete access to PRTG Network Monitor via the web. Use the PRTG web interface as default interface to setup your monitoring and bring it to perfection.

Configure devices and sensors, set up notifications, review monitoring results, create reports, visualize your monitoring on dashboards, and use many more PRTG features to complete your monitoring.

The PRTG web interface is based on Asynchronous Java Script and XML (AJAX) and designed to optimally adjust to your systems by its **responsive design**. It shows all object setting dialogs as pop-up layers, so you never lose the current context. The web interface adjusts to the size of your screen, so you always get information displayed in an optimized way.

While you are [logged in](#)^[168], the PRTG web interface continuously refreshes the data on the screen via AJAX calls and you always are up to date on the current monitoring results. You can [set](#)^[3376] the refresh interval and method individually.

Thanks to **Single Page Application (SPA)** technology, your system will stay highly performant because only single page elements are refreshed when necessary.

The following sections introduce the features and concepts of the Ajax Graphical User Interface (GUI).

 If you are interested in a video overview of the PRTG web interface, see this video tutorial: [The PRTG Web User Interface—Overview](#)

Ajax Web Interface—Basic Procedures—Topics

- [Login](#)^[168]
- [SSL Certificate Warning](#)^[172]
- [Welcome Page](#)^[175]
 - [Customer Service](#)^[178]
- [General Layout](#)^[181]
- [Sensor States](#)^[195]
- [Review Monitoring Data](#)^[198]
- Compare Sensors
- [Historic Data Reports](#)^[204]
- [Similar Sensors](#)^[209]
- [Recommended Sensors](#)^[213]
- [Object Settings](#)^[217]
- [Alarms](#)^[219]

- [System Information](#)  222
- [Logs](#)  228
- [Tickets](#)  230
- [Working with Table Lists](#)  237
- [Object Selector](#)  240
- [Priority and Favorites](#)  242
- [Pause](#)  245
- [Context Menus](#)  247
- [Hover Popup](#)  262
- [Main Menu Structure](#)  263

Other Ajax Web Interface Sections

- [Ajax Web Interface—Device and Sensor Setup](#)  280
- [Ajax Web Interface—Advanced Procedures](#)  3184

Related Topics

- [Enterprise Console](#)  3430
- [PRTG Apps for Mobile Network Monitoring](#)  3484

6.1 Login

For PRTG on premises instances, you can log in to the web interface once the PRTG core server is [installed](#)^[89]. In your browser, load the IP address or DNS name of the computer PRTG is installed on and log in using the **Login** button. For PRTG hosted by Paessler instances, open your registered PRTG hosted by Paessler domain and log in to the web interface.

You can look up and change the web server settings of PRTG on premises instances at any time using the [PRTG Administration Tool](#)^[362] Windows application on the system where the PRTG core server is installed. Especially when accessing PRTG from the internet, you should use an SSL-encrypted connection. You can easily switch to SSL using the **Yes, switch to SSL** button shown on the welcome screen.

Loading the Web Interface

In a web browser window, please enter the IP address or URL of the system PRTG is installed on. When using a cluster, please connect to the primary master node. You can also double-click on the **PRTG Network Monitor** icon on the desktop of the system PRTG is installed on. If you are using PRTG hosted by Paessler, enter the URL of your instance, for example [myfirstdomain.my-prtg.com](#) to access the web interface with a [supported browser](#)^[31].

 If you run PRTG on localhost, please do not use the DNS name [http://localhost](#) to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or [http://127.0.0.1](#) instead.

If you see a certificate warning in your browser, you can usually just confirm it. For more information please see [SSL Certificate Warning](#)^[172].

Login Screen PRTG on Premises

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

After loading the web interface, the login screen is visible. You can either login as default administrator or as any other PRTG user. As **PRTG Administrator** user you can use all functionalities of the web interface. Administrators can [create additional users](#)^[376] with administrator rights or with more restricted privileges (for example, read-only users).

PRTG Network Monitor

Login Name

Password

Login

> Download Client Software (optional, for Windows, iOS, Android)
> Forgot password? > Need Help?

PRTG NETWORK MONITOR

Paessler Blog

Learn, Workshop and Discuss: Why You Should Atte...
Hands-on Workshops, Serverless Architecture and Webpack For the second time in a row, we decided to participate in the Nuremberg Web Week and to share our knowledge about modern web applications with the local developer scene. This

PRTG Podcast: How to Clean Up after WannaCry
As a follow up to the first ever, recently released PRTG podcast (which, if you haven't listened to already, you may need to re-assess your life choices - click here immediately!), Rupert Collier, our resident UK sales manager and aspiring

How Automatic Inventory Can Make Your Life Easier...
Companies need a complete overview of their own IT infrastructure. The rapid pace of change requires the inventory overview to be frequently updated. Using Excel spreadsheets to maintain the inventory overview is limiting: inflexible, error-prone.

It's Time for Your SysAdmin Day Resolution: Invest i...
SysAdmin Day is coming up on Friday, July 28th. This year, how about celebrating the day (and the coming year) with a resolution to invest in yourself to boost your skills and advance your career? Making a commitment to professional development

Why You Should Enable HTTPS on Your Website (Ye...
There are Many Reasons in Favor of HTTPS and None (Really) Against It

PRTG Login Screen

Login as Default Administrator (First Time Login)

This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

When logging in for the first time, login name and password for the default administrator login are both **prtgadmin**. PRTG automatically fills in the default credentials and shows the password in plain text.

- After login you should change the default password. To do so, go to **Set up | Account Settings | My Account** and specify a new password in section **User Account**.
- If you are not logged in into the web interface, you can change the credentials for this default user account any time in the [PRTG Administration Tool](#)³⁵⁷⁴ Windows application.
- If you enter another login name or change your password, the password is no longer shown in plain text.

Login as PRTG User

This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

If you have received user credentials from your administrator, please enter them here to log in. Also, when using other administrator credentials, please enter them here.

Login Options

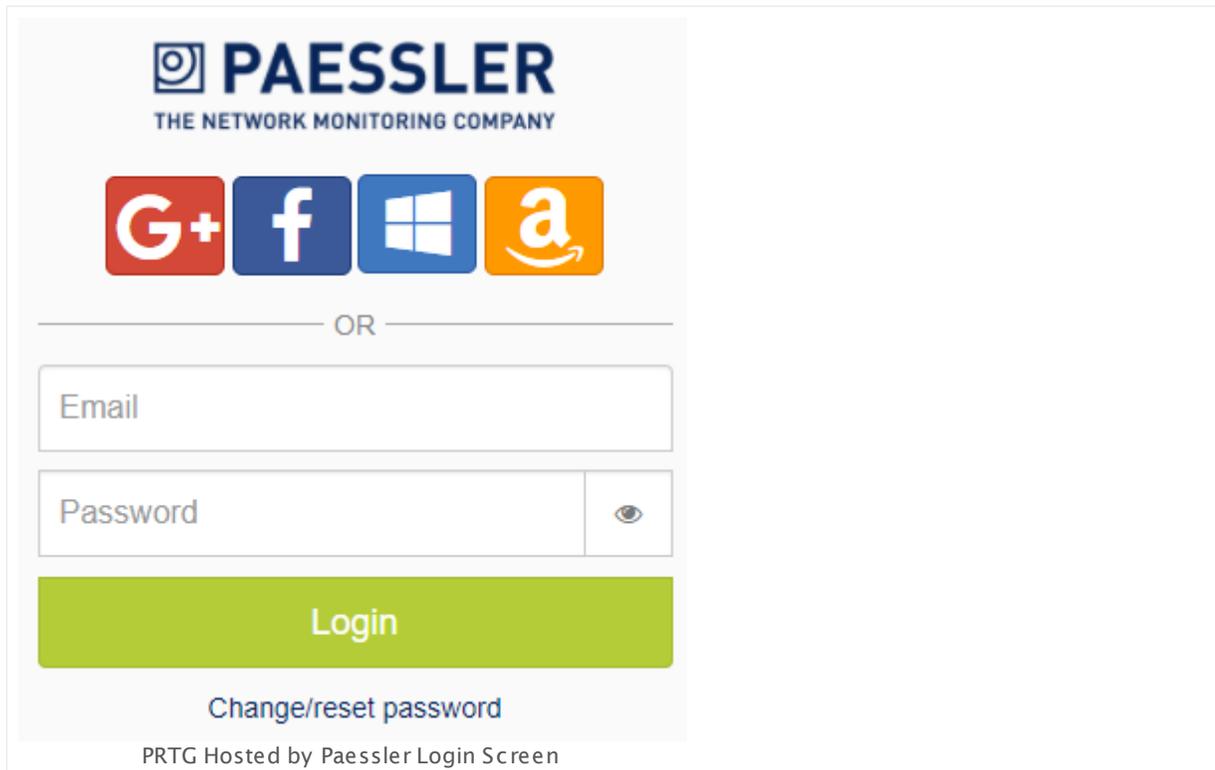
This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

- **Login:** Log in to the fully featured Ajax web interface, which is the standard interface. We recommend that you use this option for PRTG whenever possible. It offers the full functionality of PRTG. Use Google Chrome 67 or later (recommended) or Mozilla Firefox 61 or later for best performance. In some browsers, the Ajax option is not shown, for example, in old browser versions.
- ❗ Although you can log in using Microsoft Internet Explorer 11, the Ajax web interface might **not** be fully compatible with Internet Explorer! When using Microsoft Internet Explorer 11, please set the security level to **Medium-high** (or lower) and make sure no **Compatibility View** is enabled!
- **Download Client Software (optional, for Windows, iOS, Android):** This option opens the PRTG [download page](#)^[3420] in the web interface. You can optionally download the native Windows application **Enterprise Console** to the desktop. You have to [install](#)^[3430] it on the client computer before use. The [Enterprise Console](#)^[3430] provides full functionality. However, for some functions the Ajax Web GUI opens. As an additional feature, the Enterprise Console can view data of several independent PRTG core installations in one single application.
 - ❗ Also, when using this download option, your name and password (or the default credentials) are required for login!
- ❗ Only Google Chrome 67 or later (recommended) and Mozilla Firefox 61 or later are fully compatible with the Ajax web interface.

Enter specific credentials or use the default credentials, which are automatically filled in, and click the **Login** button to proceed to the PRTG web interface.

Login Screen PRTG hosted by Paessler

For PRTG hosted by Paessler instances, load the PRTG web interface with the domain you have registered at <https://my-prtg.com> and use the login method that you chose when signing up.



The image shows the PRTG login screen. At the top, the Paessler logo is displayed with the tagline 'THE NETWORK MONITORING COMPANY'. Below the logo are four social media icons: Google+, Facebook, Windows, and Amazon. A horizontal line with the word 'OR' in the center separates these icons from the login fields. There are two input fields: 'Email' and 'Password'. The 'Password' field has a small eye icon to its right. Below the input fields is a large green 'Login' button. Underneath the button is a link that says 'Change/reset password'. At the bottom of the screen, it says 'PRTG Hosted by Paessler Login Screen'.

To log in with Facebook, Google+, Windows, or Amazon, click the respective button. A popup window appears where you can enter your credentials for the respective account. Alternatively, you can log in with the email and password that you chose when signing up. If you have received an invitation to PRTG hosted by Paessler, click the link in the invitation and proceed to log in.

Recover Password

If you cannot remember your PRTG on premises password, click the **Forgot password?** link. The **Password Recovery** page opens. Enter your **Login Name**, click **Request a New Password**, and PRTG will send a new password to the primary email address of this PRTG user account. The **Need Help?** link will open the current manual page.

If you cannot remember your PRTG hosted by Paessler password, click the **Change/reset password** link. You are then asked to enter your email address. Click **Change/reset password** again and PRTG will send you an email to reset your password.

6.2 SSL Certificate Warning

If you use PRTG on premises outside your internal LAN, especially when you use it on the internet, you should [switch the internal web server to use SSL](#)^[172]. After doing so, your browser shows a certificate warning because the certificate that comes with PRTG cannot be signed by a valid authority. Anyway, the connection to your PRTG web server is secured via SSL, and you can confirm the claimed security risk.

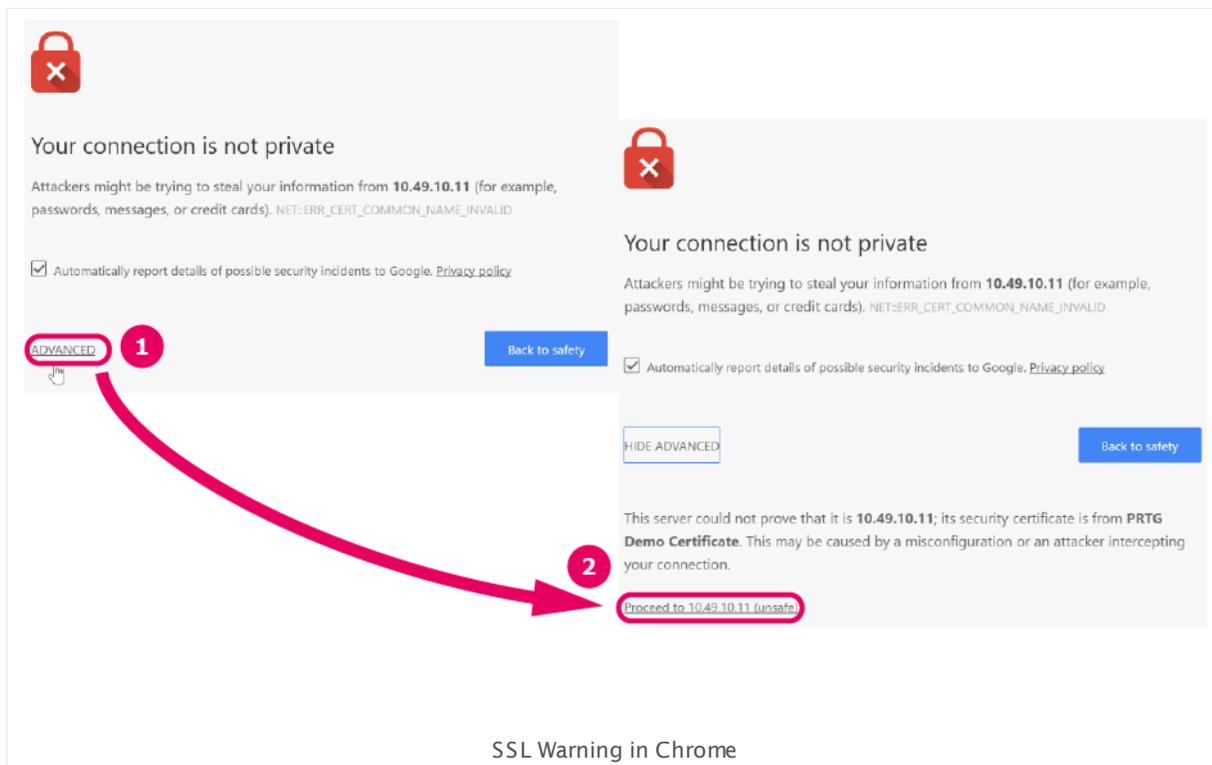
Every browser shows a slightly different certificate warning. The necessary steps are similar for every browser, with a few small differences:

- [Google Chrome](#)^[172]
- [Mozilla Firefox](#)^[173]
- [Internet Explorer](#)^[173]
- [Other](#)^[174]

You can avoid these browser warnings by [using your own trusted SSL certificate](#)^[376] with PRTG. For this purpose we provide the freeware tool [PRTG Certificate Importer](#)^[376].

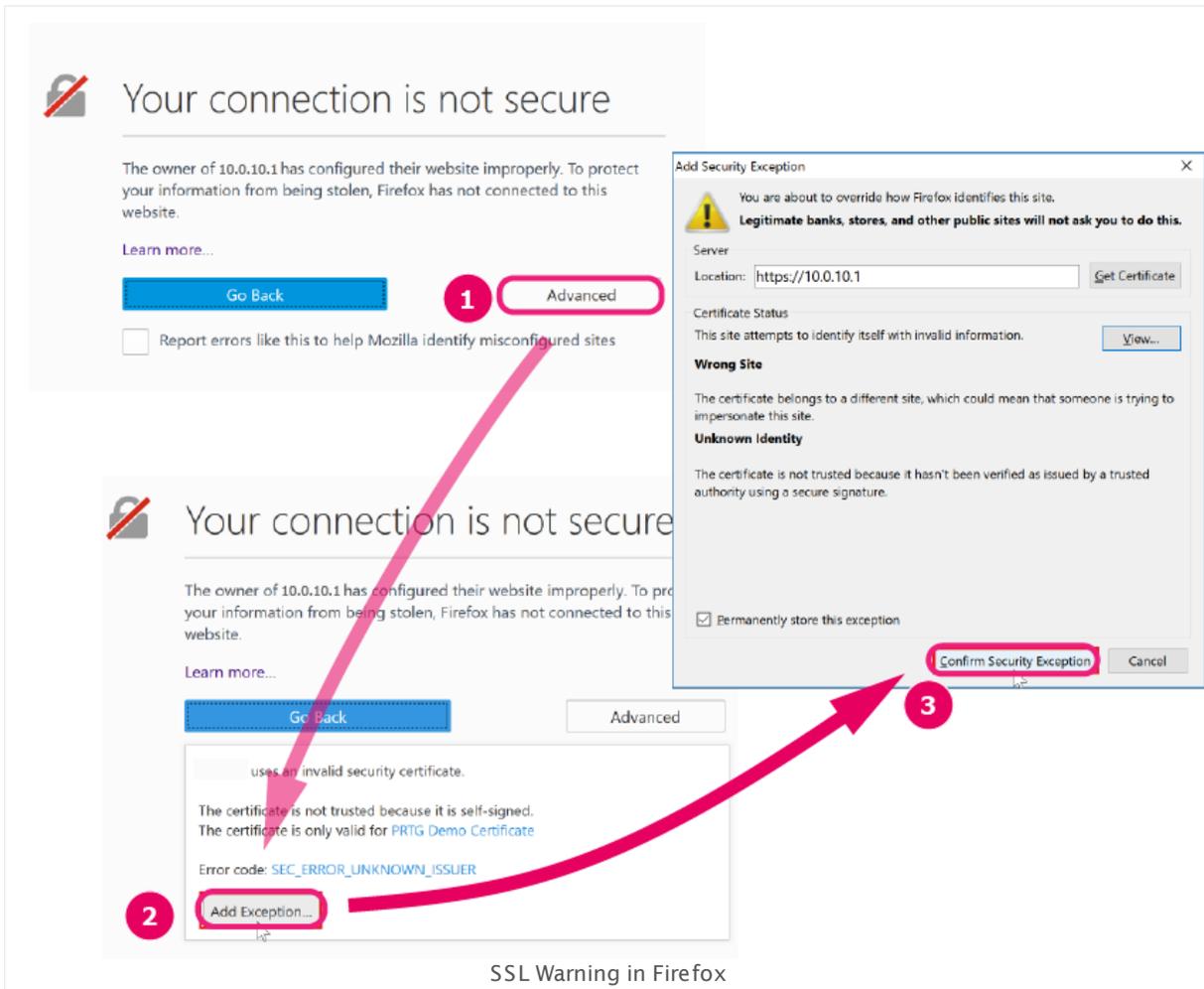
Google Chrome

In **Google Chrome**, click **Advanced** and then **Proceed to [yourPRTGserver] (unsafe)** every time you call the PRTG web interface.



Mozilla Firefox

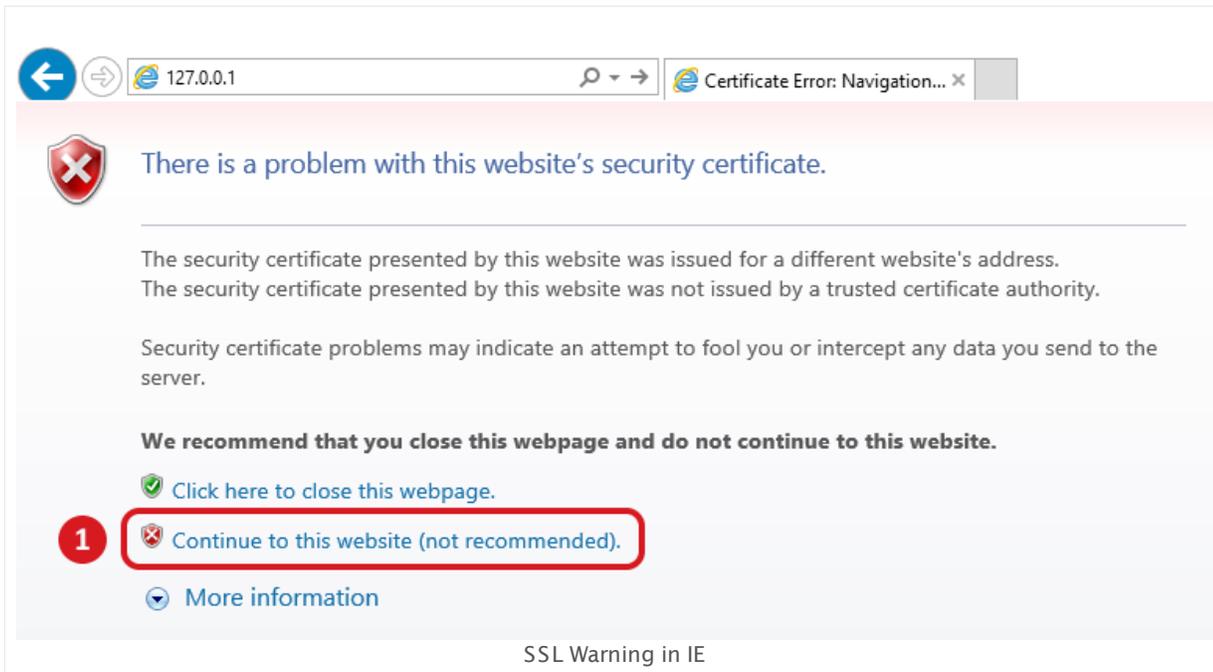
In **Mozilla Firefox**, click **Advanced** and then click the **Add Exception...** button. A window opens, leave the check mark for **Permanently store this exception** and finally click the **Confirm Security Exception** button.



You only have to go through this procedure once for every Firefox browser and PRTG core server.

Internet Explorer

In **Internet Explorer**, click **Continue to this website (not recommended)** every time you call the web interface.



Other

For other, not officially supported browsers, the procedure is similar.

More

- [Using Your Own SSL Certificate](#) 

Freeware Network Tools: PRTG Certificate Importer—Installing Trusted SSL Certificates for PRTG Network Monitor

- <https://www.paessler.com/tools/certificateimporter>

Knowledge Base: Why can't I save my PRTG password in Google Chrome?

- <https://kb.paessler.com/en/topic/61982>

6.3 Welcome Page

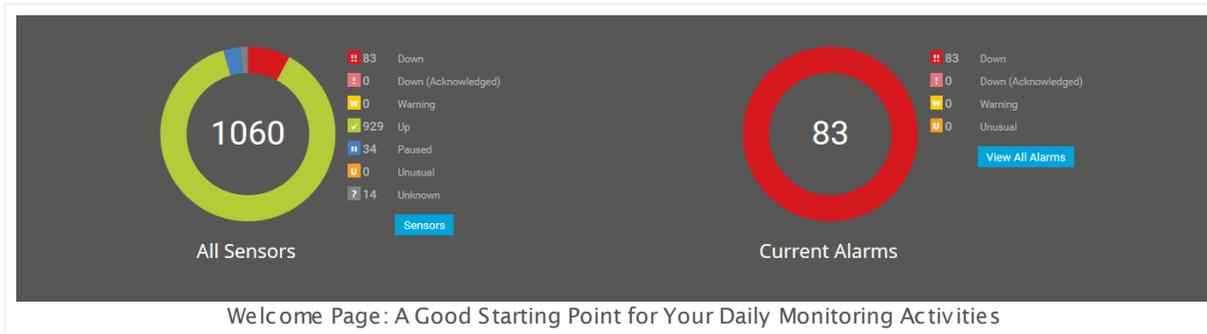
After completing the [Smart Setup](#)^[52], you will see PRTG's welcome page by default when you log in to the web interface. You can set another homepage in your [account settings](#)^[3304], section **Web Interface**.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

The PRTG welcome page shows you various information about your PRTG installation at a glance, similar to a dashboard. The welcome page keeps you informed about all [Sensors](#)^[267] and current [Alarms](#)^[219]:

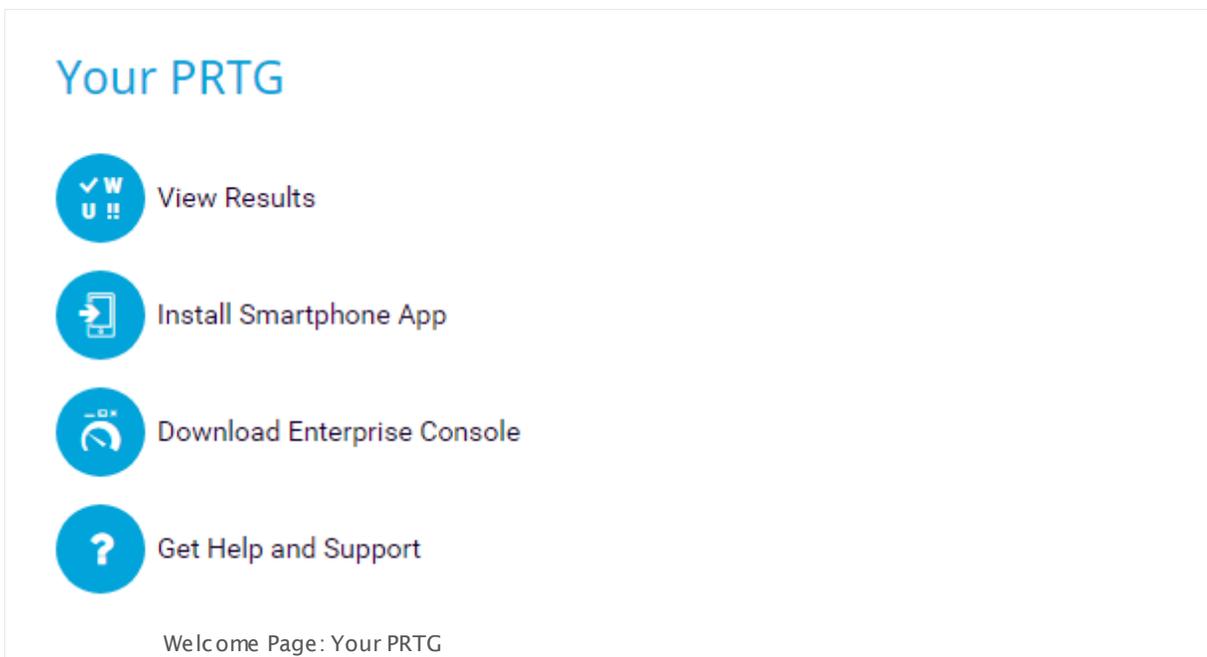
- **Sensors:** Open the [Top 10 Lists](#)^[267] for sensors.

- **View All Alarms:** Open a [list of alarms](#) in your PRTG installation.



You can also directly access several pages in the PRTG web interface from the welcome page:

- **View Results:** Open the [device tree](#) that shows your monitoring results.
- **Install Smart phone App:** Open the [download page for PRTG's mobile apps](#).
- **Download Enterprise Console:** Open the [download page for the Enterprise Console](#) in PRTG (PRTG on premises only).
- **Get Help and Support:** Open the PRTG help and support page from where you can access the PRTG user manual, the Knowledge Base, and video tutorials. You can also open [support tickets](#) and contact [our customer service](#) from this page.
- **Manage Subscription:** Open your PRTG hosted by Paessler dashboard and manage your subscriptions.



Other sections are:

- **Paessler Blog:** Shows recent information about PRTG and Paessler. Click the heading of an article to open it on paessler.com with your browser.

- **Yesterday's Activity:** Shows what your PRTG server did for you on the day before. Point with your mouse to the mini graph to show the number of sensor scans on a specific day. See also manual section [PRTG Status—System Status](#)^[3400], section **Activity History**.
- **License Status:** Shows the number of your remaining maintenance days for PRTG on premises and the number of sensors you can still add with your current license. Click **Get Maintenance** to open the Paessler shop and extend your maintenance for PRTG on premises installations. Click **Get More Sensors** to open the Paessler shop and upgrade your license. See also manual section [PRTG Status—License Status and Settings](#)^[3414].
 - ❗ The number of available sensors that is displayed here does not consider [paused sensors](#)^[245] for technical reasons. However, paused sensors do not count against the maximum number of sensors that your license allows. Add the number of your paused sensors to the displayed number to know exactly how many sensors are still available on your installation.
 - ❗ If you use a PRTG on premises license with an unlimited number of sensors, PRTG takes 10,000 sensors as starting point to calculate the number of available sensors, which is displayed here. Please consider the [system requirements](#)^[26] for a properly working PRTG setup and click **Recommended Setup** for more information.
- **Update Available:** Shows the version number of your PRTG on premises core server and the version number of the latest available PRTG version. You will see the label **NEW** if there is a newer version available. Click **Install Update** to open the PRTG [Auto-Update](#)^[3407] page.
- If your PRTG on premises installation is currently not SSL-secured, the welcome page will ask you to enable SSL encryption for the PRTG website. Click **Yes, Switch to SSL** to enable SSL encryption or **Don't Tell Me Again** to remove this note from the welcome page. See also manual section [System Administration—User Interface](#)^[3346].
- If you still use the default password of the PRTG System Administrator user (**prtgadmin**) on a PRTG on premises installation, the welcome page will ask you to set a secret password if your PRTG website is publicly accessible. Click **Change Default Password Now** to define a new password. See also manual section [System Administration—User Accounts](#)^[3377].
- In the **video section** you find informative and helpful videos about monitoring with PRTG. Click a video to open and play it on paessler.com.

The collected information about your PRTG installation makes the welcome page a good starting point for your daily monitoring activities. Of course, you can also set up your custom dashboards in PRTG. The [Maps](#)^[3276] feature of PRTG enables you to create dashboards exactly like you want.

6.3.1 Customer Service

If you have any questions about license purchase, upgrade, or maintenance extension, you can directly contact the Paessler **Customer Service** from the **Help and Support Center** in the PRTG web interface. We will readily assist you with quotes or information about licensing and maintenance, and guide you through the purchasing process. Our Customer Services team will also gladly send you the contact information of a knowledgeable PRTG partner in your region or research any technical specifications you might need beforehand.

 PRTG transmits your feedback or questions securely to Paessler via the PRTG Cloud. Please make sure your PRTG server has access to the internet and can reach the URL <https://api.prtgcloud.com:443> for successful transmission.

Contact Paessler Customer Service / Send Your Feedback to Paessler ✕

[Ask a Question or Give Us Your Feedback](#)

Your Name

John Q. Public

Your Email Address

JohnQPublic@company.com

Your Country

Deutschland (Germany) ▼

Your Phone Number

+49

How can we help?

Information on licensing

Need a quote

Need contact to a Technical Presales Engineer

Need contact to a partner/reseller in my country

Other

Emotional State

OK ▼

[Cancel](#) [Submit](#)

Customer Service Contact Form

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the **Contact Paessler Customer Service** form:

- **Your Name:** Enter your full name for contact information.
- **Your Email Address:** Enter an email address under which we can reach you.

- **Your Country:** Select the country in which you run PRTG so we can provide you contact information for a partner near you.
- **Your Phone Number:** Enter a phone number under which we can reach you.
- **How can we help?** Select the scope of your question.
- **Emotional State:** If you want to, you can indicate your current feelings about PRTG and your purchase process.
- **Describe your question in one sentence:** Provide short information that indicates the topic of your request.
- **Do you have any further comments?** Enter your comments here. This can be feedback or any questions for our customer service.

Click **Submit** to send your question or feedback to our customer service. Click **Cancel** to close the customer service contact form without sending it.

 If you have technical questions regarding your already existing PRTG setup, [contact our technical support](#).

6.4 General Layout

This manual section provides a general overview of the structure of the web interface of PRTG. Central focus is the **Devices** view, which you can select via the main menu bar. The **Devices** view presents the monitoring results at a glance—you will widely use it.

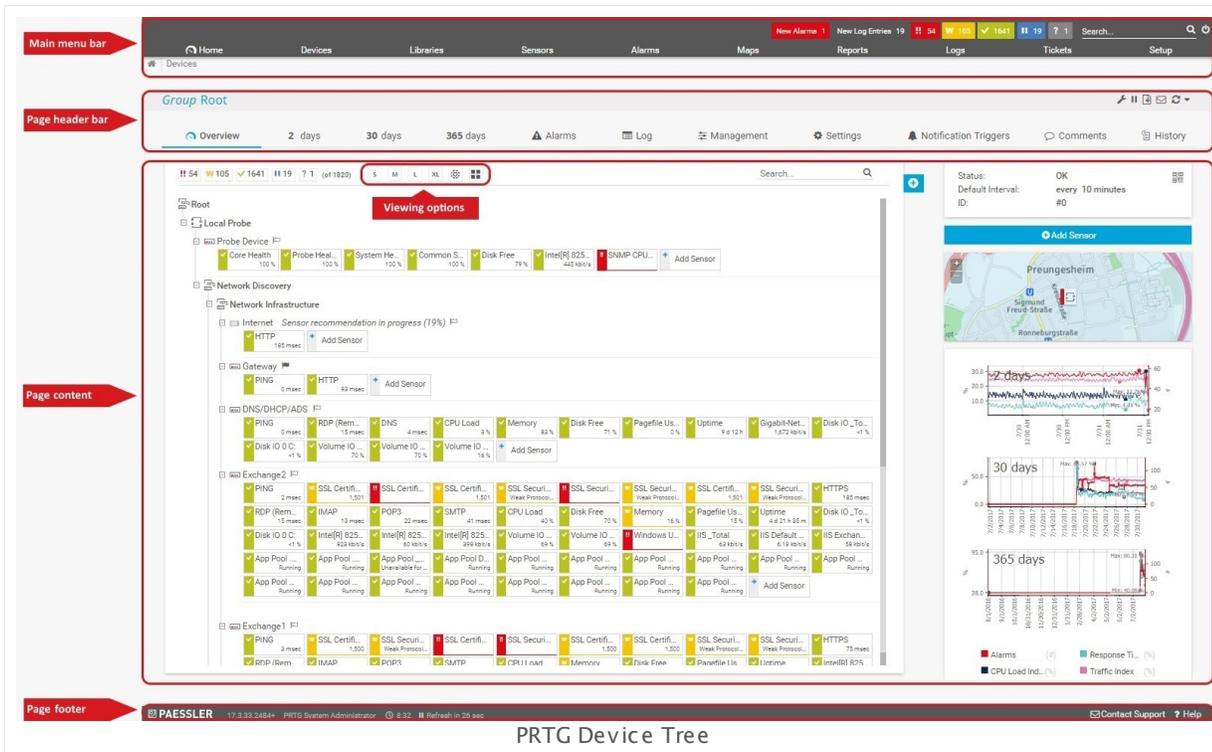
Welcome Page

When you log in to the PRTG web interface, by default you will see the [Welcome Page](#)^[175]. You can set another homepage in your [account settings](#)^[3304], section **Web Interface**.

Click **View Results** to open the device tree window.

Tree View Layout

Click **View Results** on the welcome screen to display the device tree window. This will be a good starting point for your everyday work with PRTG.



From top to bottom, the device tree screen has several areas that will be covered in further detail in this section. For a general overview of the device tree consider the table below.

Page area name	Description
Global Header Area ¹⁸⁵	This area contains the main menu at the very top, the global status bar, the path to the currently selected object, and a quick search box.
Page Header Bar ¹⁸⁵	This area contains the page heading with the name of the current object, several tabs with settings, monitoring data of the current object, and quick action buttons.
Page Content ¹⁸⁶	This area contains information about the current object and all other objects underneath in the tree hierarchy, the object's status bar, a quick search box, and the QR code that links to the current URL.
Viewing options ¹⁸⁷	These buttons are part of the page content. Here you can adjust how your device tree is displayed.
Page Footer	Shows information about the current version of PRTG, the logged in PRTG user account, and the current time (depending on the timezone settings ³³⁸⁰ for the currently logged in user). A timer counts down how much time remains until the next automatic page refresh. You can pause the refresh timer with the pause icon and resume with the play icon. If you open another page while the refresh timer is paused, the timer will resume automatically, starting with the defined Auto Refresh Interval that you can configure in your account settings ³³⁰⁷ .  Long table lists ²³⁷ that are set to display 1000 items at a time will be excluded from automatic refresh to ensure system performance.
Page Footer Icons	With these icons you have quick access to the PRTG Auto-Update ³⁴⁰⁷ page if a new version is available and to the contact support form ³⁴²⁴ . There is also a link to context sensitive help. When running PRTG in a cluster, you will also see a cluster related element. It shows the name of the node that you are logged in to and displays whether this is a master or a failover node. Click the bar to show the Cluster Status ³⁴¹² . In a failover node, you can review all data, but changes in the settings will not be saved. In order to change settings, please log in to the master node of your cluster.

Click an object to see its details page. In the page heading of the [page header bar](#) ¹⁸⁵ you always see the name of the object that you have currently selected.

When navigating the PRTG web interface, the following paths are available:

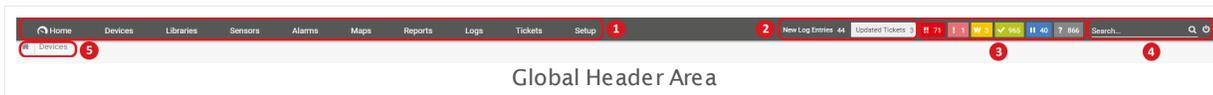
- The main menu provides access to all important aspects of the software.
- The quick search is often the fastest way to find a specific object (for example, a sensor or a device).

- Using the page tabs, you can switch between various sub-pages.
- Right-clicking objects will open a [context menu](#)^[247].
- When pausing over objects, the tool tip appears, and after further hovering a quick-access window ([Hover Popup](#)^[262]) will open.
- You can drill down into the object hierarchy of probes, groups, devices, and sensors in the object tree by merely clicking a sub-object of the currently displayed object (for example, a sensor on the device page).

These navigation paths offer complete access to the functionality of PRTG, often you will find multiple means of accessing information or navigating to a certain setting.

In the following, the different areas of the web interface are described.

Global Header Area



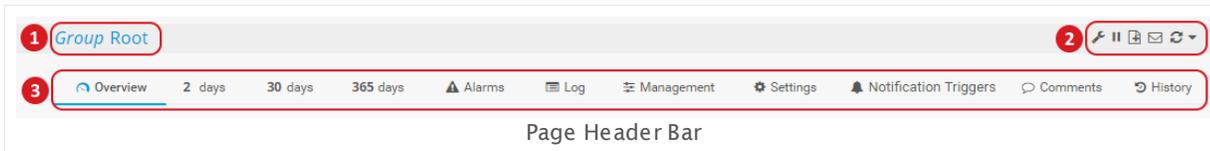
The header area of the web interface provides central, very condensed information about your installation and offers access to all content and every setting within PRTG. The following table lists the elements that the global header area is made up of.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Screen Number	Part	Description
1	Main Menu Bar	For starting to navigate through the web interface, the main menu is the best starting point. We recommend that you take a few minutes to familiarize yourself with the menu bar and its sub-items. For a detailed description see the Main Menu Structure ^[263] section.
2	New Alarms, New Log Entries, New Tickets	The information boxes show how many new alarms, new log entries, and updated tickets have occurred. Click the respective box to view the lists of Alarms ^[219] , Logs ^[228] , or Tickets ^[230] .
3	Global Sensor Status Symbols	This area shows the accumulated states of all sensors you have configured for monitoring, divided according to the different sensor states. Depending on each respective status, you will see colored boxes with numbers that symbolize the amount of sensors that are in the respective status. For example, you can see how many sensors are in Up , Down , or Warning status. Click a box to view a list of all sensors in the respective status. For a detailed description, see the Sensor States ^[195] section.
4	Search Bar, Logout	<p>Via the icons in the top-right corner you can start a search or log out.</p> <p>To search for a monitoring object, enter a name, parts of a name, an IP address, a DNS name, or a tag in the search box on the right and confirm with enter. PRTG will perform a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments.</p> <p>A page with the items that are related to the search term will open—even displaying online help articles.</p>
5	Breadcrumbs	Below the main menu, PRTG shows a path that retraces the steps back to the welcome screen (or your defined starting page). Use it to quickly jump back to where you came from. Breadcrumbs can also help you to orient yourself if you get lost. If you click a breadcrumb item, a dropdown menu opens that shows all objects on the same level. You can either search for an object, or select one directly. For example, you can use this to directly access all other sensors or a device, other devices within a group, and another group on the same probe. Other probes in your root group are also available.

Page Header Bar

The page header bar, below the global header area, consists of a number of elements shown in the table below.



Screen Number	Part	Description
1	Page Heading	This line displays the current object's type and name as page heading. In the screenshot above, it is a group that is called Root . Here you can define the object's priority by clicking on one of the five stars (not available for the Root group). For details, see section Priority and Favorites ^[242] .
2	Context Buttons	On the right side is a row of icons for several actions. Depending on the currently viewed page within PRTG, you can pause (and resume) the respective object. You can also add another object (for example, a sensor to a device), send a link to the current page per email, perform an immediate scan, open a related ticket, or show the corresponding object history page ^[229] . Click the down arrow to open the context menu for the currently displayed object for further options. For more information, see Context Menus ^[247] section.
3	Tabs	Via tabs you can navigate to the various sub-pages of an object, for example, to its monitoring data or settings. For more information, see sections Review Sensor Data ^[198] and Change Device and Sensor Settings ^[217] .

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Depending on the selected object type, the page header bar shows additional information:

- All objects underneath the Root group show their [dependency](#)^[141].
- Groups and devices display the time elapsed since the last execution of the [auto-discovery](#)^[282] on the selected object.

Part 6: Ajax Web Interface—Basic Procedures | 4 General Layout

- Devices show their respective DNS/IP address as defined in the [device settings](#)^[402] and the time elapsed since the last execution of the [sensor recommendation](#)^[213] on this device.
- Sensors show additional monitoring statistics.

Page Content

The page content of the general layout varies dependent on the selected object. It shows information about the current object and all other objects underneath in the tree hierarchy. The deeper down in the hierarchy you select an object, the more detailed is the displayed information.

The screenshot displays the PRTG Network Monitor interface. On the left, a tree view shows the hierarchy: Root > Local Probe > Probe Device > Core Health (100%), Probe Health (100%), System Health (100%), Common S... (100%), Disk Free (79%), Intel[R] 825... (466 kb/s), and SNMP CPU... (red). Below this, 'Network Infrastructure' is expanded to show 'Internet F2' with HTTP (141 msec), 'Gateway gw' with PING (0 msec) and HTTP (54 msec), 'DNS/DHCP/ADS: dc1 F2' with PING (2 msec), RDP (Rem...) (10 msec), DNS (6 msec), CPU Load (2%), Memory (82%), Disk Free (71%), Pagefile Us... (5%), and Uptime (9 d 17 h), and 'Exchange F2' with a large grid of sensors including PING, SSL Certifi..., RDP (Rem...), IMAP, POP3, SMTP, CPU Load, Disk Free, Memory, Pagefile Us..., Uptime, Disk IO, Intel[R] 825..., and multiple App Pool sensors.

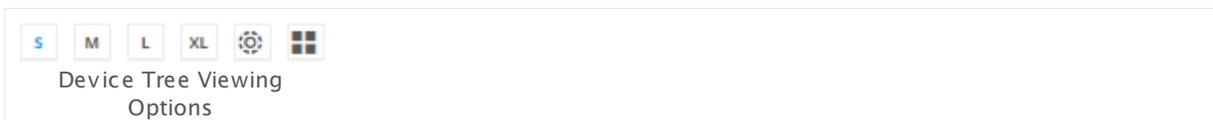
On the right, a detailed view of a sensor is shown. It includes a status box (Status: OK, Default Interval: every 10 minutes, ID: #0), a map of 'Preungesheim', and three time-series charts for 7 days, 30 days, and 365 days. A legend at the bottom identifies the data series: Alarms (red square), Response TL... (green square), CPU Load Ind... (blue square), and Traffic Index (pink square).

Page Content

1	Sensor Status Bar	<p>This element is visible when viewing a probe, a group (including Root), or a device. It is not available when the sensor details page is open. The sensor status bar shows the accumulated states of all sensors for the current object, divided into different sensor states. They show the number of sensors in the respective status.</p> <p>For example, you can see how many sensors are in Up, Down, or Warning state. For a detailed description of sensor states, see the Sensor States^[195] section. You can hide sensors that are in a certain state by removing the check mark in front of the respective status. To show them again, re-add the check mark.</p>
2	Viewing options	<p>This element is only visible when viewing a probe or a group. It is not available when you view device or sensor details. For a detailed description, see Switch Device Tree View^[187] below.</p>
3	Tree Search	<p>In the white search box to the right of the tree view selection, enter a key word to search the device tree for matching items. The tree will highlight matching devices and sensors by graying-out all others. This can help to gain a quick overview over sensors monitoring a specific part of your network. For example, you can enter the keyword "firewall" to highlight devices and sensors matching this name.</p>
4	Add Button	<p>Use this button to add new objects to your monitoring setup. For a detailed description, see Add Button^[192] below.</p>
5	Object Status, Scanning Interval, Object ID, QR Code	<p>This element displays the current status of the selected object, the time interval in which PRTG scans the current object, the ID of the current object, and the QR code for the current page. If you use a PRTG mobile app^[3494], you can scan the code to view the current object directly on your mobile device. Click the QR code to enlarge it for scanning.</p>

Switch Device Tree View

Wherever a probe or group is displayed, you can choose between a number of viewing options.



Switch Device Tree View—Classic Device Tree

Via the sizes in the page header bar, you can adjust how much information will be included next to each object. Using the various buttons, you can switch from a very condensed view (SM) to an extra spacious view (XL).

In the classic device tree view you can **collapse** devices, groups, and probes. Click the minus box left of the object name. The sensor states will then be summarized. The states of all sensors on this object will be displayed. Right next to the status, the amount of sensors in this status will be displayed, with the exception of the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**. In the default settings, the sensors will be grouped together if there are more than ten sensors with the same status, otherwise they will be displayed individually.

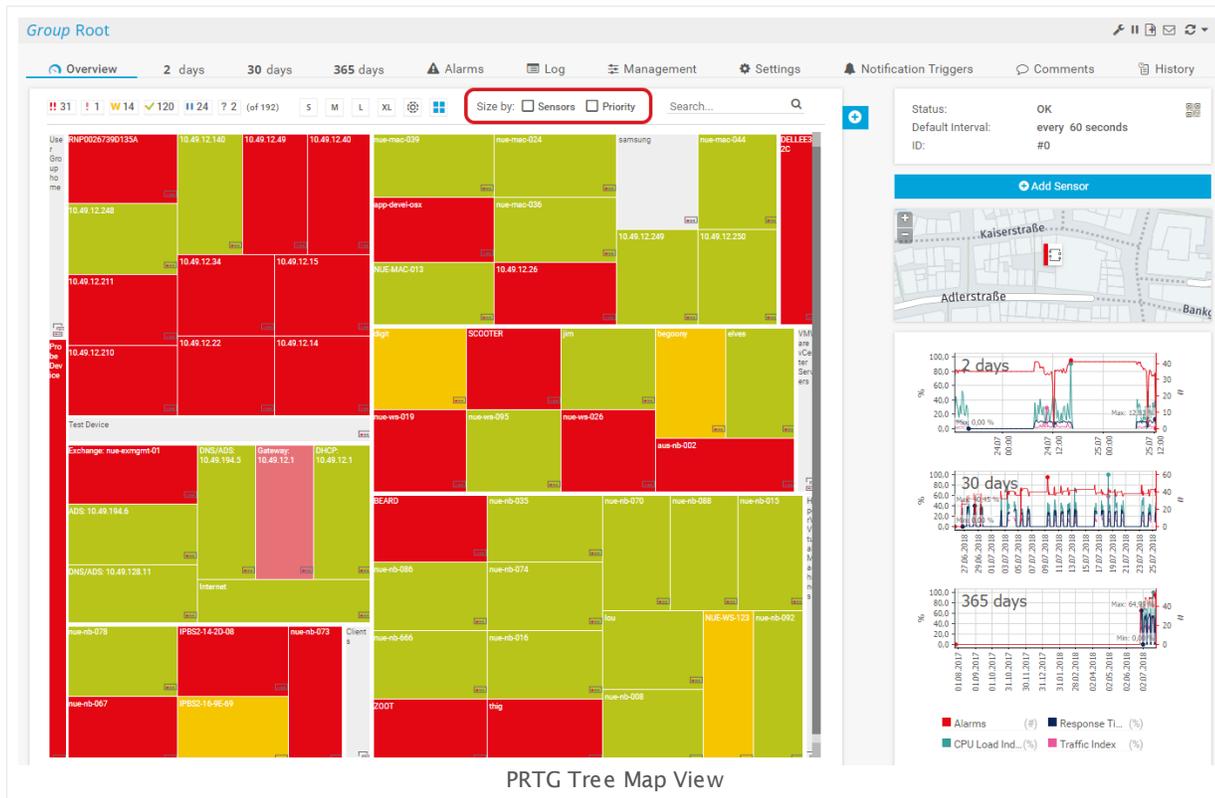


Switch Device Tree View—Extended Views

There are two additional options to the simple tree views that enable you to display the status of all sensors of your entire installation in a single overview. Choose one of the icons to change the view:

Tree Map View (6)

The tree map view displays all devices of your entire installation as tiles sorted into a square and arranged according to the groups they belong to. Each device dynamically changes color to reflect the overall status of the sensors on the device. You can also adjust the square size: either depending on a device's priority, or depending on the number of sensors on a device, or depending on both. To do this, click the **Size by: Sensors** and/or **Priority** setting in the page header bar (see the mark in the screenshot below).



Sunburst View (5)

The sunburst view displays your entire installation as a circle diagram. The groups are represented as inner circles, and all devices contained within a group are shown as 'cake slices' attached to the outside of a circle element.

The sunburst is interactive:

- You can click elements to open the details view of your monitoring objects.
- You can zoom in and out by using the plus + and minus - buttons or your mouse wheel.
- You can change the position of the sunburst on the overview tab with drag & drop.

Flag	Flag Color	Object Status	Meaning
	Red	Down	At least one sensor 'belonging to' this object shows a red Down status. Point to an object's name to view the total number of alarms concerning this object.
	Bright-Red	Down (Acknowledged)	At least one sensor belonging to this object is Down and the status has been acknowledged by a PRTG user via the Acknowledge Alarm function. All of this device's Down states must have been acknowledged—if at least one sensor is not acknowledged, this object will be displayed as Down .
	Yellow	Warning	At least one sensor belonging to this object shows a yellow Warning status. There is no sensor in a Down or Down (Acknowledged) status concerning this object.
	Orange	Unusual	At least one sensor belonging to this object shows an orange Unusual status. There is no sensor in a Down , Down (Acknowledged) , or Warning status concerning this object.
	Green	Up	All sensors belonging to this object are in a green Up status. There is no sensor in a Down , Down (Acknowledged) , Warning , Paused , or Unusual status concerning this object.
	Blue	Paused	All sensors belonging to this object show a blue Paused status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , or Up status concerning this object.
	Black (Grey)	Unknown	All sensors belonging to this object have an Unknown status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , Paused , or Up status concerning this object.

▪ **Size by Sensors / Size by Priority**

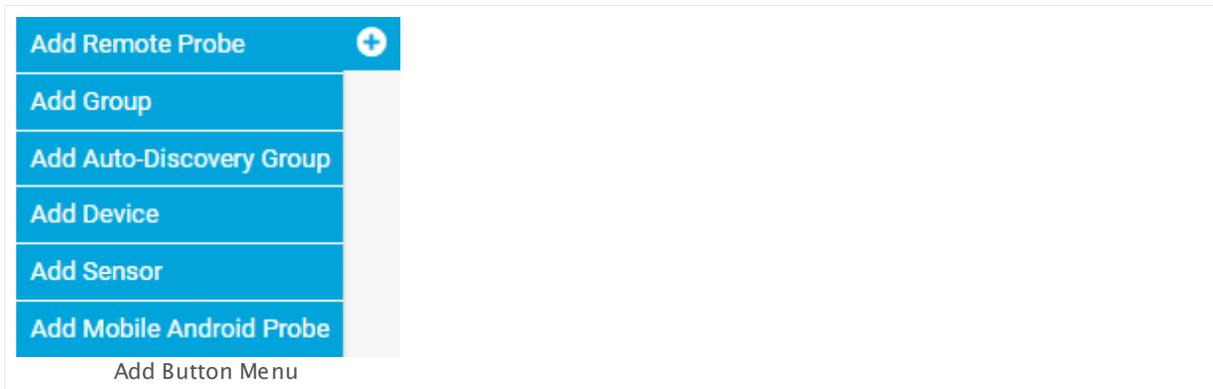
You can adjust the size of the different squares. They can be calculated by the amount of sensors running on a device or within a group, or by the sensors' priority (see [Priority and Favorites](#)^[242]), or both. Use the check boxes in the page header bar (see below) to change the view immediately, then use the setting that suits you best.

Size by: Sensors Priority
 Sorting Checkboxes

Add Button

Hover over  to add new objects to your monitoring setup. An assistant will appear, leading you through the necessary steps.

 The content of the PRTG context menu varies, depending on the menu item or tab you have selected.



See the following for more information:

- [Add Remote Probe](#)  3707
- [Add a Group](#)  302
- [Auto-Discovery—Creating an Auto-Discovery Group](#)  283
- [Add a Device](#)  311
- [Add a Sensor](#)  325
- [Add Mobile Android Probe](#)

Default Objects in the Device Tree

By default, a **Probe Device** is created in the device tree on the [local probe](#)  3742 or [hosted probe](#)  3743. It represents the probe system running with your PRTG installation. PRTG automatically monitors the system health of the core server and each probe to discover overloading situations that may distort monitoring results. To monitor the system status of the probe computer, PRTG automatically creates a few sensors:

- [Core Health Sensor](#)  652
- [Probe Health Sensor](#)  1590
- [System Health Sensor](#)  2669
- Some further device specific sensors for disk usage and bandwidth

In a cluster installation, PRTG also creates a **Cluster Probe Device** with a [Cluster Health Sensor](#)  638 that monitors the cluster's system health.

We recommend that you keep these sensors, but they all are removable.

6.5 Sensor States

In the PRTG device tree you usually create several sensors for each [device](#)^[402]. With sensors, you can monitor different aspects of your devices. Using a simple color code, they always show you what is going on in your network.

The color of a sensor always shows its current status. In the below table, you will find a list of states a sensor can show. This list also reflects the hierarchy of states whenever summarized sensor states are shown (in the [device tree](#)^[181], or on [geo maps](#)^[3211]): the higher a status is in the hierarchy, the higher will be its priority in displaying sensor states. For example, if all the sensors of a specific device are **Up**, but one of its sensors reaches a **Down** status, then the overall status of this device will be **Down** as well (for example, displayed red in the [Tree Map View](#)^[187]), because this status is higher up in the hierarchy.

i **Down** and **Down (Partial)** states are equal in the status hierarchy.

Sensor	Color	Status Name	Meaning
	Red	Down	<ol style="list-style-type: none"> 1. PRTG is unable to reach the device, or the sensor has changed to the error state. See the Sensor Warning and Down Behavior^[196] below for more information. <ul style="list-style-type: none"> i By design, a sensor does not record any data in its channels while it shows this status. 2. Another reason for this status can be an error limit that is set in the Sensor Channels Settings^[3160], or an error status due to a sensor Lookup^[3693]. <ul style="list-style-type: none"> i In this case, the sensor continues to record data in all sensor channels although the sensor shows an error.
	Green/Red	Down (Partial)	<p>In a cluster, at least one node reports this sensor as Down, while at least one other node reports the same sensor as Up.</p> <ul style="list-style-type: none"> i This status is not available for sensors on remote probes in a failover cluster^[130].
	Bright-Red	Down (Acknowledged)	<p>The sensor is Down and the status was acknowledged by a PRTG user, applying the Acknowledge Alarm function. This can be helpful to mark that an alarm has already been brought to attention. For acknowledged alarms no further notifications^[3216] are sent. To set this sensor status, right-click the sensor in Down status and from the context menu^[247], select Acknowledge Alarm... Then enter a comment and click OK.</p>

Sensor	Color	Status Name	Meaning
	Yellow	Warning	The sensor gives an error reading, but PRTG will try again. The sensor may soon change to a down status. See the Sensor Warning and Down Behavior ^[196] below for more information. Another reason for this status can be a warning limit set in a sensor's Sensor Channels Settings ^[3160] .
	Orange	Unusual	The sensor reports unusual values for this weekday and time of day. The unusual detection is based on the historic average data and can be configured or disabled in the system administration ^[3356] . You can also disable unusual detection for certain groups only (see Group Settings ^[399]).
	Green	Up	The last scan was okay and the sensor currently receives data.
	Blue	Paused	The sensor is currently paused (for a certain timespan, indefinitely, or triggered by a dependency ^[141]).
	Black (Gray)	Unknown	The sensor has not received any data yet or there is an error in (network) communication, likely on the probe system. If sensors show this status persistently, a PRTG restart may be necessary.  For extended troubleshooting, see this Knowledge Base article: What to check if sensors are black (gray)?

Sensor Warning and Down Behavior

The **Down** status symbolizes that something is wrong with a monitored device. There can be various reasons for a down status, for example, an interruption in the physical connection to the device, an internet connection outage, or a crashed server.

After a failed request, PRTG tries to re-contact the device before setting a sensor to **Down** status (this is true for almost all types of sensors):

1. If a request to a device fails for the first time, the sensor will change to **Warning** status. PRTG repeats the request and attempts to re-scan the device immediately.
2. If the second request also fails, the sensor changes to **Down** status by default until the device is reachable again. You can change this behavior in the [Scanning Interval](#)^[343] settings of any monitoring object. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are informed promptly about any network issues.

 The behavior described above does **not** apply to **Warning** or **Down** states that are activated due to a warning or error limit set in the [Sensor Channels Settings](#)^[3160] or to channels using [lookups](#)^[3693].

More

Video Tutorial: The PRTG Sensor States

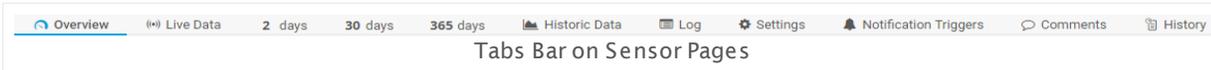
- <https://www.paessler.com/support/videos/prtg-basics/sensor-states>

Knowledge Base: What to check if sensors are black (gray)?

- <https://kb.paessler.com/en/topic/25643>

6.6 Review Monitoring Data

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Overview

The **Overview** tab shows an overview of the currently selected object and its sensors. The pages share a common structure, but some elements differ, depending on the type of object.

- **Probes and Groups:** the tab shows a tree-like view with devices and sensors, a Geo Map, as well as summary graphs for different timespans of the current probe or group.
- **Devices:** the tab shows device details, a Geo Map, and summary graphs for different timespans, colored gauges for high priority sensors, as well as a table list of all sensors on this device, and a [table list](#) [237] with [Recommended Sensors](#) [213].
- **Sensors:** the tab shows sensor details, current status, colored gauges, sensor graphs for different timespans, a table with all sensor channels, as well as [similar sensors](#) [209], which show correlations in your network.

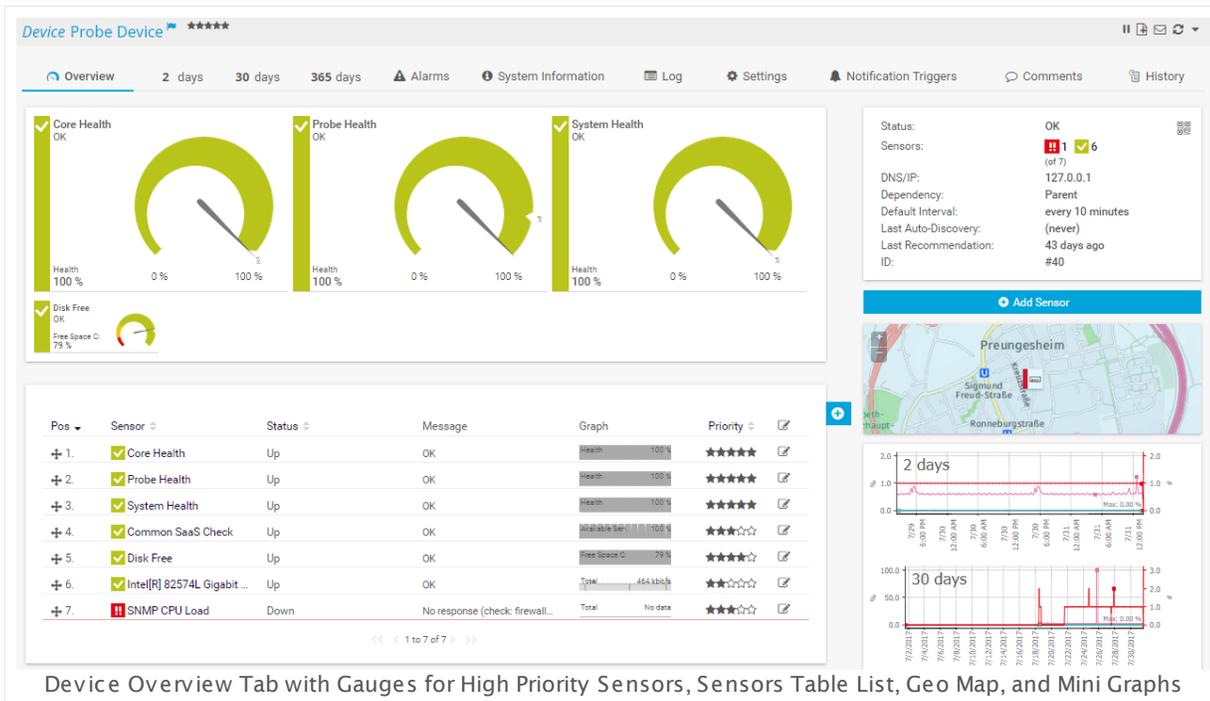
i You can turn off the sensor recommendation and disable the table list in [System Administration—Monitoring](#) [3369].

i Assign 4 star (***) or 5 star (****) priorities to sensors to display their gauges on your device overview pages. 5 star sensors are represented by larger gauges (upper row on the screenshot) rather than 4 star sensors (lower row on the screenshot).

Gauges represent sensor values on the **Overview** tab of devices and channel values on **Overview** tabs of sensors. They visualize the current value of a sensor or a channel, so you can use them as a quick status indicator.

- Red and yellow sections of gauges correspond to the error and warning limits of the [sensor channel settings](#) [3160].
- Device overview tabs only show gauges of high priority sensors, sensors with priorities of 3 stars (***) or less are omitted here.
- Sensor overview tabs show gauges of all sensor channels (except the **Downtime** channel), regardless of priority. The primary channel is displayed with the large gauge.
- Sensor channels that display binary values such as on/off or successful/failing due to their [lookup](#) [3693] configuration are visualized as **switches** not gauges. Switches only show red or green for their respective two states.

i For the gauge to remain legible, we recommend that you stay below 120 [lookup](#) [3693] values for primary channels, which belong to sensors with a 5 star priority. For sensors with a priority of 4 stars, the recommended limit is around 40 lookup values.



Toplists

Toplists are available for [xFlow and Packet Sniffer sensors](#)^[430] only. Toplist graphs are displayed right on the sensor overview page.

For more information, see the section [Toplists](#)^[3186].

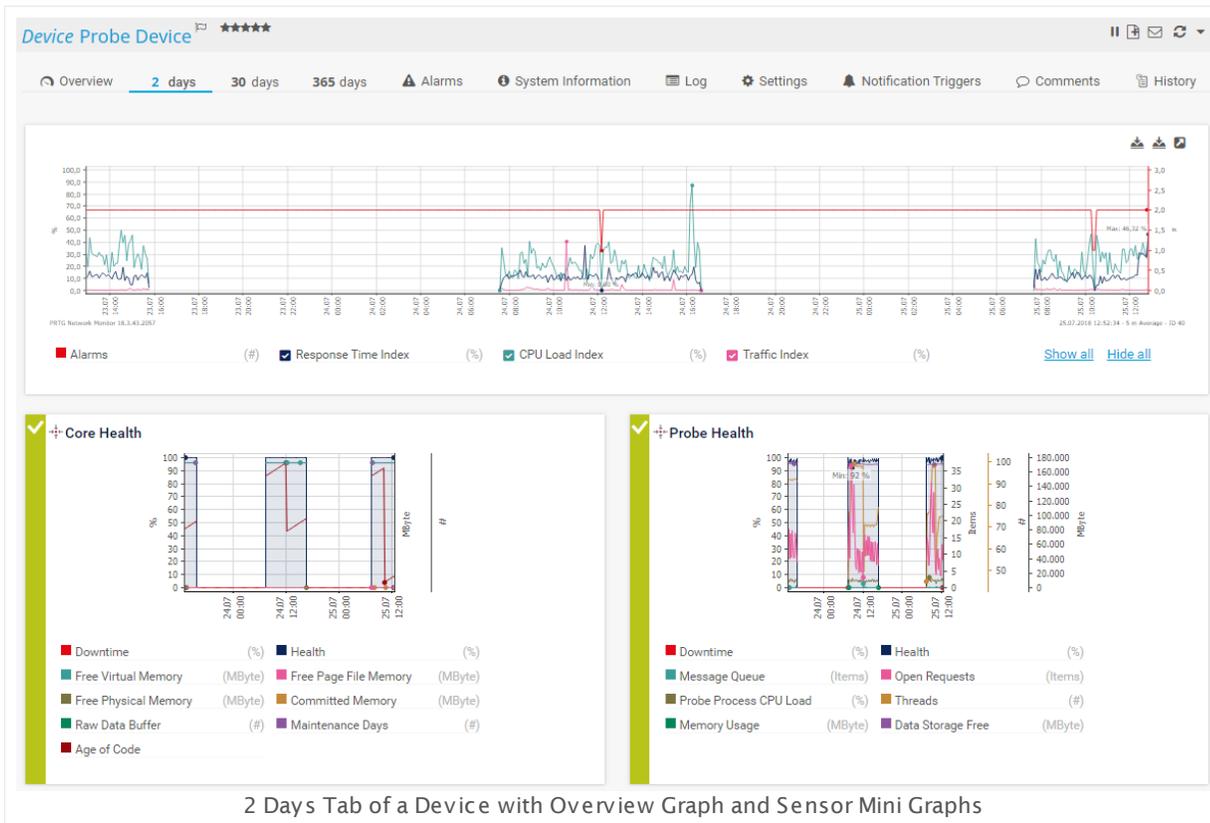
Live Data and Data By x Days

Select one of the tabs **Live Data** (available for sensors only), **2 days**, **30 days**, or **365 days** to display an object's monitoring data live (sensors only), or for different timespans and in more or less detail. The time that graph legends and data tables show depends on the [time zone settings](#)^[3380] for the currently logged in user.

The days mentioned here is the default setting. You can change the shown days of the different graphs under [System Administration—User Interface](#)^[3351].

Graphs label minimum and maximum values of a sensor's primary channel and minimum and maximum values of the **Response Time Index** of other objects. A maximum value of 100% will not be labeled.

Part 6: Ajax Web Interface—Basic Procedures | 6 Review Monitoring Data



Live Data and Data By x Days—Probes, Groups, and Devices

For probes, groups, and devices, each of the tabs shows a summary graph for the current object and mini graphs for all sensors on this object, as well as a data table for the current object. For performance reasons, PRTG never displays more than 50 mini graphs. Hover over a mini graph to display the graph legend.

Summary graphs show the number of alarms as well as three **index graphs**. These graphs indicate response time, CPU usage, and bandwidth usage for all sensors. Index graphs are similar to a stock index. The shown values are based on the readings of all sensors of this object. PRTG computes these values using statistics and by comparing the values to the highest and lowest readings ever recorded.

The three index graphs show overall (or global) trends in your network. If these values increase over a specific time frame, then CPU load, bandwidth load, or response time respectively have worsened during this time. For example, a **CPU Load Index** value of 90% means that the average CPU load for all CPU sensors of your current configuration is at 90% of the highest ever measured CPU usage value.

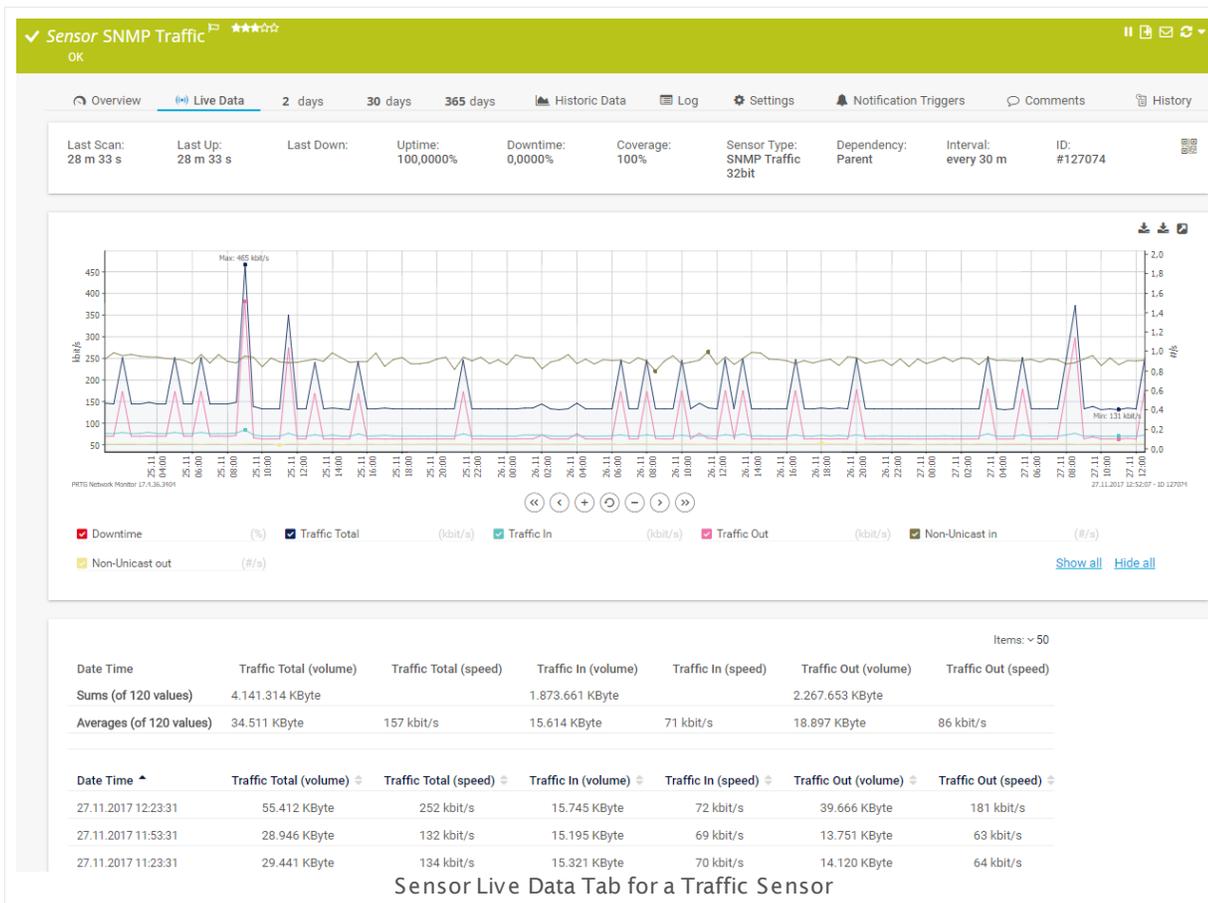
The following four channels are available in the summary graph:

- **Alarms:** Sums up the number of all down states of sensors on this object during the given time span. This graph provides you a bird's eye view of your network issues. It cannot be hidden.
- **Response Time Index:** Indicates the request times in your network.

- **CPU Load Index:** Indicates the CPU usage in your network.
- **Traffic Index:** Indicates the bandwidth usage in your network.

 For more details about the index graphs, see the Knowledge Base: [How does PRTG compute CPU Index, Traffic Index and Response Time Index?](#)

You can hide all channels individually except the "Alarms" channel. To do this, remove the check mark symbol in front of a channel name besides the graph, and the corresponding channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons below the channel names. The graph view will be reset immediately.



The screenshot displays the 'Sensor SNMP Traffic' interface. At the top, there's a green header with the sensor name and status. Below it, a navigation bar includes 'Overview', 'Live Data' (selected), and other options like '2 days', '30 days', '365 days', 'Historic Data', 'Log', 'Settings', 'Notification Triggers', 'Comments', and 'History'. A summary row provides key metrics: Last Scan (28 m 33 s), Last Up (28 m 33 s), Last Down, Uptime (100,000%), Downtime (0,000%), Coverage (100%), Sensor Type (SNMP Traffic 32bit), Dependency (Parent), Interval (every 30 m), and ID (#127074).

The main section features a line graph showing traffic over time. The y-axis represents traffic in kbit/s (0 to 450) and #/s (0.0 to 2.0). The x-axis shows dates from 25.11.2017 to 27.11.2017. A legend below the graph allows toggling various data series: Downtime (%), Traffic Total (kbit/s), Traffic In (kbit/s), Traffic Out (kbit/s), Non-Unicast in (#/s), and Non-Unicast out (#/s). There are 'Show all' and 'Hide all' buttons.

Below the graph is a table with columns for Date Time, Traffic Total (volume), Traffic Total (speed), Traffic In (volume), Traffic In (speed), Traffic Out (volume), and Traffic Out (speed). The table shows summary data for 'Sums (of 120 values)' and 'Averages (of 120 values)', followed by a list of individual data points for the last few minutes.

Sensor Live Data Tab for a Traffic Sensor

Live Data and Data By x Days—Sensors

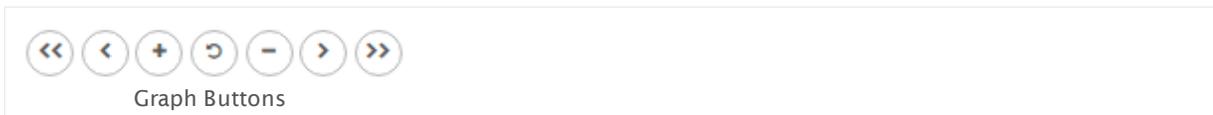
For sensors, each tab shows a graph and data table for the selected sensor. When viewing the data of a sensor running on a cluster probe, you can additionally select if you want to show the data of all nodes, or of one specific node only. Please use the **Select Cluster Member** bar below the tabs.

 Multi-node graphs are never displayed as filled graphs, but are displayed with lines only. However, historic data reports can have filled multi-node graphs.

While viewing a sensor graph you can hide single sensor channels individually. Simply remove the check mark symbol in front of a channel name below the graph, and the according channel's line will disappear. You can also **Show all** or **Hide all** channels by clicking on the buttons besides the channel names.

Live Data and Data By x Days—Interactive Graphs

The graphs on a sensor's historic data tabs and in "zoomed graphs in new windows" (see below) belonging to other monitoring objects are all interactive. You can zoom in and scroll along the time axis with the corresponding buttons.



The following actions are available for graphs:

- **<<** scrolls one graph window left and **>>** one graph window right. The scrolled time depends on the graph you select, for example, 2 days on a 2 days graph.
- **<** scrolls left and **>** right on the time axis. The scrolled time depends on the graph you select.
- **+** zooms into and **-** out of the graph. The displayed time depends on the graph selected. For example, you can zoom in a 30 days graph so that it shows data for 6 days.
- **x** resets the graph to the default view.

In the upper right corner of each graph, three small icons are located   :

-   **Download the graph (PNG or SVG):** Shows a PNG or SVG file of the graph in a new browser window. You can then save or copy it for later use.
-  **Zoom graph in new window:** Opens a larger version of the graph in a new browser window.

For each graph, you can also choose which specific channels (only on sensor pages) or indexes you want to see via the corresponding check boxes or the **Show all** and **Hide all** buttons.

 [Warning or error limits](#)^[3162] are only shown in graphs (highlighted in yellow or red) if you select exactly one channel with a limit.

Historic Data

The **Historic Data** tab is available for sensors only.

 For more information, section [Historic Data Reports](#)^[204].

Sensor Lists

Viewing lists of sensors is a great way to keep an eye on your network status because you can select which kind of sensors you would like to see. There are many different sensor list views available, such as a list of favorite sensors and top 10 lists, lists filtered by current sensor status, value, availability, tag or type, sensor cross reference, and many more.

Sensor lists are accessible via the main menu bar. Click the **Sensors** entry to show a table list of all sensors. In the [table list](#)^[237] displayed here, you can re-arrange the items by clicking the column's header items (see section [Working with Table Lists](#)^[237]). Hover over it to show other menu options.

 For detailed information about the available options, see the [Main Menu Structure](#)^[267] (**Sensors**) section.

Alarms

The **Alarms** tab is not available for sensors, but for probes, groups, and devices only.

 For more information, see the [Alarms](#)^[219] section.

System Information

The **System Information** tab is available for devices only.

 For more information, see section [System Information](#)^[222].

Log

The **Logs** tab shows past activities and events regarding the currently selected object.

 For more information, see the [Logs](#)^[228] section.

Related Topics

- [Object Settings](#)^[217]

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

6.7 Historic Data Reports

For quick reviews of a sensor's monitoring data, use the historic data reports as an alternative to the comprehensive [Reports](#) ³²⁵² function. You can run and view a report of the historic data for each single sensor, on demand. Additionally, you can export this sensor data as XML or CSV files to your computer for further processing with third-party applications.

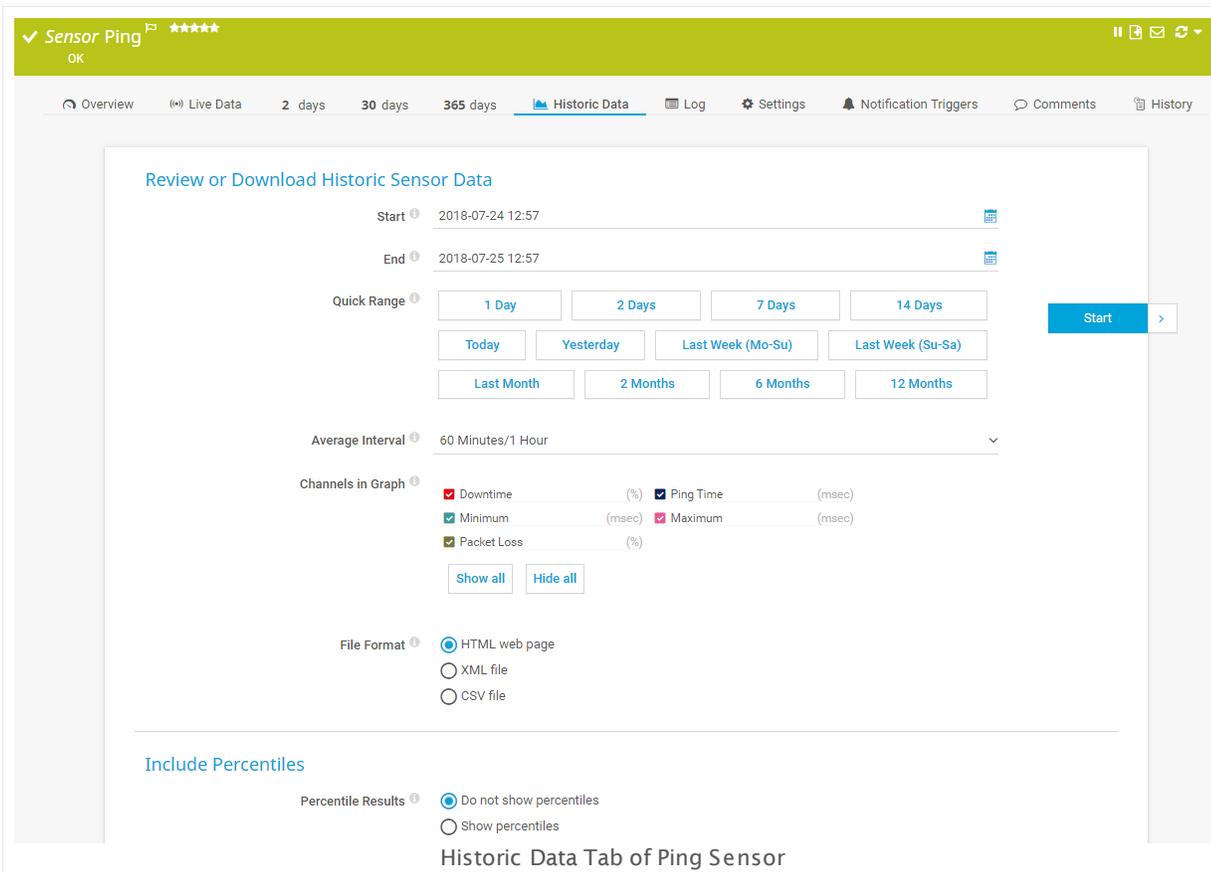
There are two ways to open PRTG historic data reports: either you click the **Historic Data** tab on a sensor's detail page, or you choose **Sensors | View Historic Data** from the [main menu](#) ²⁶⁷.

Historic Data (Sensor Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When you open the historic data tab of a sensor, there is no sensor selection available. If you want to select a different sensor for the report, select **Sensors | View Historic Data** from the main menu in the PRTG web interface.



Historic Monitoring Data (Sensors Main Menu)

When you open historic data reports via **Sensors | View Historic Data** in the main menu, PRTG will ask you to choose the sensor you want to create a report for with the [Object Selector](#)^[240].

Historic Monitoring Data Settings

SETTINGS	
Sensor	This field is only visible if you open the historic data function via the main menu. Select the sensor you want to create the report for: click the reading-glass symbol to open the object selector. For more information, see section Object Selector ^[240] .
Start	Specify the start date and time of the data you want to review. Use the date time picker to enter the date and time. i You cannot start the report generation if monitoring data has been purged ^[3373] after the defined start date. Please set the start for the report to a date where data is available.
End	Specify the end date and time of the data you want to review. Use the date time picker to enter the date and time.
Quick Range	In this section you can use several buttons for a faster selection of start and end dates. Click any of these links to change the Start and End values above. Choose between: <ul style="list-style-type: none"> ▪ 1 Day, 2 Days, 7 Days, or 14 Days: Set the date range to the respective day(s). The current time of the current day is the end date. ▪ Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, 12 Months: Set the date range to the last matching period. It starts at 00:00 and ends at 00:00 of the particularly following day.
Average Interval	With this option, you can activate and configure averaging. Select an interval for which PRTG will calculate the average value. You can choose between No Interval (no averaging is performed and only raw data displayed), a few seconds, minutes, hours, or a whole day (24 Hours). A shorter interval results in a more detailed report for this sensor. The best settings for you may vary, depending on the scanning interval of the sensor, the selected date period, and the intended use for the report. It might be useful to try different settings and compare what the results look like.

SETTINGS

 See the section [Automatic Averaging](#)  below.

Channels in Graph

Select the channels that you want to include in the graph of the report. You can select or deselect individual channels with the respective check boxes, and select or deselect all channels with the buttons **Show all** or **Hide all**. PRTG will only show the data of selected channels in the graph of the report.

 The report table will always show the data of all channels.

Cluster Node

This field is only visible if the sensor is running on a cluster probe. Select the cluster node's data that PRTG will include in the report. Choose between:

- **All nodes:** Include the data of all cluster nodes in the report.
- **[Several specific nodes]:** Use a specific node's data for the report. The nodes you see are specific to your setup.

File Format

Select the output format for the report. Choose between:

- **HTML web page:** Display the result directly as HTML web page. This is also a good option to check results before exporting to another file format.
- **XML file:** Export the data as Extensible Markup Language (XML) file. Usually, your browser shows a download dialog when you use this option.
- **CSV file:** Export the data as Comma Separated Values (CSV) file, for example, for import into **Microsoft Excel**. Usually, your browser shows a download dialog when you use this option.

INCLUDE PERCENTILES

Percentile Results

Define if you want to include an additional [percentile calculation](#)  of your data in the report. Choose between:

- **Do not show percentiles:** PRTG does not use a percentile formula to calculate your monitoring results. It will show only the standard values.
- **Show percentiles:** PRTG adds a column to the result data tables that shows percentiles for every sensor channel.

INCLUDE PERCENTILES

i Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting.

Likewise, percentiles are not available in a cluster setup if you choose the option **All Nodes** in the **Cluster Node** setting in the sensor section above.

Percentile Type	<p>This setting is only visible if you select Show percentiles above. Enter the percentile type you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded.</p> <p>Please enter an integer value.</p>
Percentile Average Interval	<p>This setting is only visible if you select Show percentiles above. Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is 300 seconds (5 minutes). This means that PRTG takes 5 minute averages as basic values for the percentile calculation. Please enter an integer value.</p>
Percentile Mode	<p>This setting is only visible if you select Show percentiles above. Choose the mode for percentile calculation:</p> <ul style="list-style-type: none"> ▪ Discrete: PRTG takes discrete values to calculate percentile results. ▪ Continuous: PRTG interpolates between discrete values and bases the calculation on interpolated values.

Click **Start** to generate a historic data report.

i You cannot start the report generation if monitoring data has been [purged](#)³³⁷³ after the defined start date. Please set the start for the report to a date where data is available.

Remarks for Reports

- Any sensor graph in your report will only show channels that are enabled via the **Show in Graphs** option in the [Sensor Channels Settings](#)³¹⁶⁰.
- Reports show statistics for uptime (**Up** and **Down** in percent) and requests (**Good** and **Failed** in percent). Values between **5%** and **95%**, as well as **100%** and **0%**, are rounded to whole numbers without decimal places. Other values are shown with 3 decimal places.
- Due to rounding, the statistics in section **Sensor Status History** of the report might differ in a few seconds from the values in section **Uptime Stats**.
- Data reporting is limited to 5 requests per minute.
- Reports cannot show uptime or downtime data for the [Sensor Factory Sensor](#)¹⁷²⁰.

- Create reports that include an appropriate amount of data. Reports may not work as expected if too many sensors with short scanning intervals have to be processed. Adjust your report size and time span that the report covers if necessary.

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

TIME SPAN IN REPORT	MINIMUM LEVEL OF DETAIL (AVERAGE INTERVAL)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

Reports for time spans of more than 500 days are not possible. If you enter a longer time span, it will automatically be shortened to 365 days.

 Under certain circumstances, the resulting report may contain a time span that differs to the defined start and end date because of internal averaging processes. When averages are greater than 1 hour and they do not equal 24 hours and they are combined with certain time spans, it might happen that resulting datapoints are asynchronous to the time spans. Please especially consider this behavior when you use [API](#) calls to generate reports.

Related Topics

- [Review Monitoring Data](#)  198
- [Reports](#)  3252

More

Knowledge Base: Why is there missing data in historical data reports?

- <https://kb.paessler.com/en/topic/61382>

6.8 Similar Sensors

With PRTG you can detect relationships between different components in your network. For example, you can detect extraordinarily high CPU load correlating with extraordinarily high traffic at a specific time of a day or week. This might give you a hint to further investigate that part of your network.

What is Similarity?

The similarity calculation is based on the values that are saved in the history of sensors. If measured values change in the same way, the **similar sensors analysis** will detect it and show you the sensors that it found similar data relations for. PRTG will show all sensors that reach 85 % to 100 % similarity.

We implemented the similar sensors analysis as a heuristic calculation designed to show interconnections and correlations in your network that maybe you were not even aware of. The analysis is completely automated and sensor type agnostic. It is based on mathematics and fuzzy logic and optimizes your sensor usage by tracking redundant monitoring of some aspects of your system.

Similar Sensors Analysis in PRTG

You can adjust the depth of similar sensors analysis or turn it off in [System Administration—Monitoring](#)^[335]. You can also enable or disable the similarity analysis for specific probes, groups, and devices and specify [inheritance](#)^[137] in the corresponding [object settings](#)^[217], section **Automatic Monitoring Analysis**.

There are two options to view similar sensors:

- The overview page of sensors contains a [similar sensors section](#)^[209]. PRTG lists channels there that show similarities to channels of the current sensor.
- In addition, you can call a [similar sensors overview page](#)^[211] via **Sensors | Similar Sensors Overview** from the [main menu](#)^[267].

To edit the list of the similar sensors results, use the [available filters](#)^[212].

Similar Sensors (Sensor Overview Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



On the overview tab of a sensor, PRTG lists channels that show similarities to channels of the currently selected sensor. The table is empty if PRTG detects no similarities regarding the selected sensor.

- ❗ PRTG shows similar sensors here when channels have 85% similarity or more. The similar sensors analysis saves up to 15 entries per sensor.

Part 6: Ajax Web Interface—Basic Procedures | 8 Similar Sensors

The screenshot displays the 'Sensor SNMP Traffic' overview page. At the top, there are navigation tabs for Overview, Live Data, and historical data (2 days, 30 days, 365 days). A traffic gauge shows a total of 509 kbit/s. Below it is a table of channel statistics:

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
Traffic In	0	21,352 KByte	292 kbit/s	150 kbit/s	13,184 kbit/s
Traffic Out	1	15,923 KByte	217 kbit/s	84 kbit/s	1,824 kbit/s
Traffic Total	-1	37,275 KByte	509 kbit/s	84 kbit/s	15,007 kbit/s

The 'Similar Sensors' section, highlighted with a red box, lists three pairs of sensors with their similarity percentages:

- 100% similarity between '(011) Local Area Connection Traffic' and '(016) Local Area Connection-WFP LightWeight ...'
- 99% similarity between '(011) Local Area Connection Traffic' and '(015) Local Area Connection-QoS Packet Sched.'
- 85% similarity between '(011) Local Area Connection Traffic' and 'Intel[R] PRO_1000 MT Network Connection (To ...'

Below the similar sensors section are three graphs: 'Live Graph, 20 hours', '2 days', and '365 days', each showing traffic volume over time.

Similar Sensors Section on a Sensor's Overview Tab

The similar sensors section provides the following information:

SIMILAR SENSORS

- Similarity** Shows a measurement of similarity between two channels in percent.
- Channel** Shows a channel of the currently selected sensor.
- Similar Channel** Shows a channel of another sensor similar to a channel of the currently selected sensor (the one in the "Channel" column in the same row).

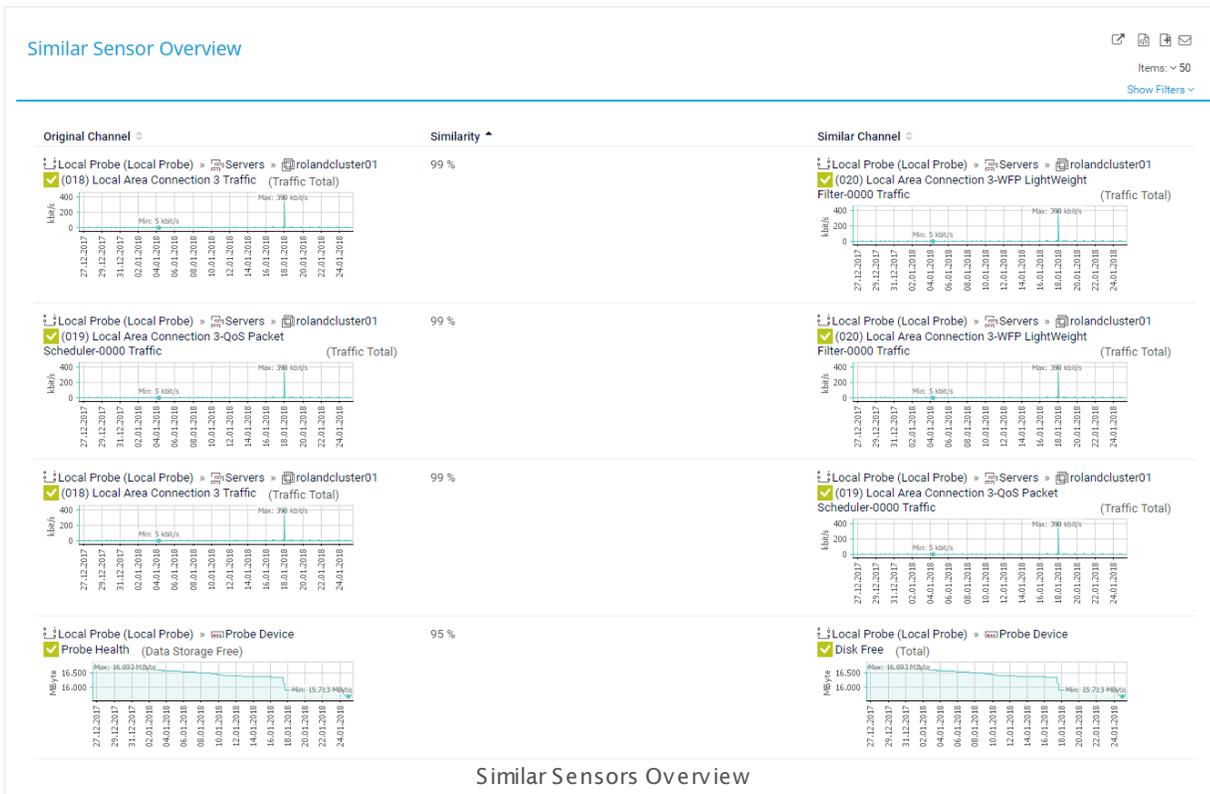
i PRTG does not show the similar sensors section when the analysis is off or when you have exceeded 1,000 sensors and selected the [automatic analysis depth option](#). You will see a notice in this case.

Similar Sensors Overview (Sensors Menu)

This page shows the results of the similar sensors analysis from the entire monitoring database. PRTG lists all channels with similarities to another one here. On the table top, you have several filter options to display similar sensors as you need it. Choose the object of interest, the degree of similarity, and if you want to display back references.

For more details, see also section [Working with Table Lists](#) ²³⁷.

PRTG shows similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor.



You can sort the list by clicking the column headers. The similar sensors overview page provides the following information:

SIMILAR SENSORS OVERVIEW

Original Channel Shows channels that other channels are compared to. Click the column header to sort the list according to the order in the device tree in ascending or descending order.

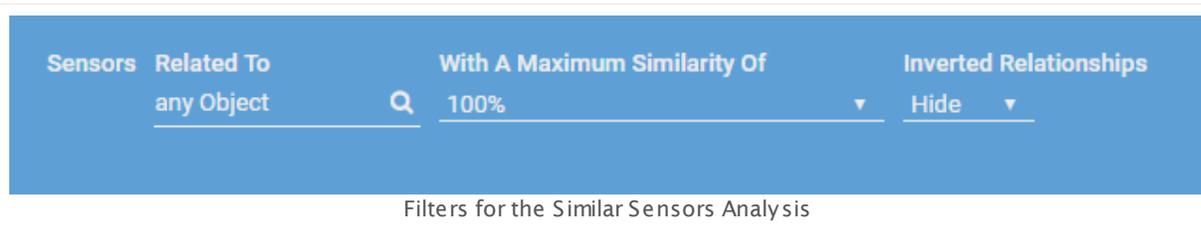
SIMILAR SENSORS OVERVIEW

Similarity	Shows a measurement of similarity between two channels in percent. Click the column header to sort the list according to the similarities in ascending or descending order.
Similar Channel	Shows a channel compared to the original channel. Click the column header to sort the list according to the order in the device tree in ascending or descending order.

i PRTG does not show the similar sensors overview option in the main menu if you turned off the analysis or if you have exceeded 1,000 sensors and selected the automatic analysis depth option.

Adjust the Similar Sensors Overview to Your Needs

You can use various filters to adjust the displayed results of the similar sensors analysis. Click **Show Filters** and edit the filters that will show up.



Filters for the Similar Sensors Analysis

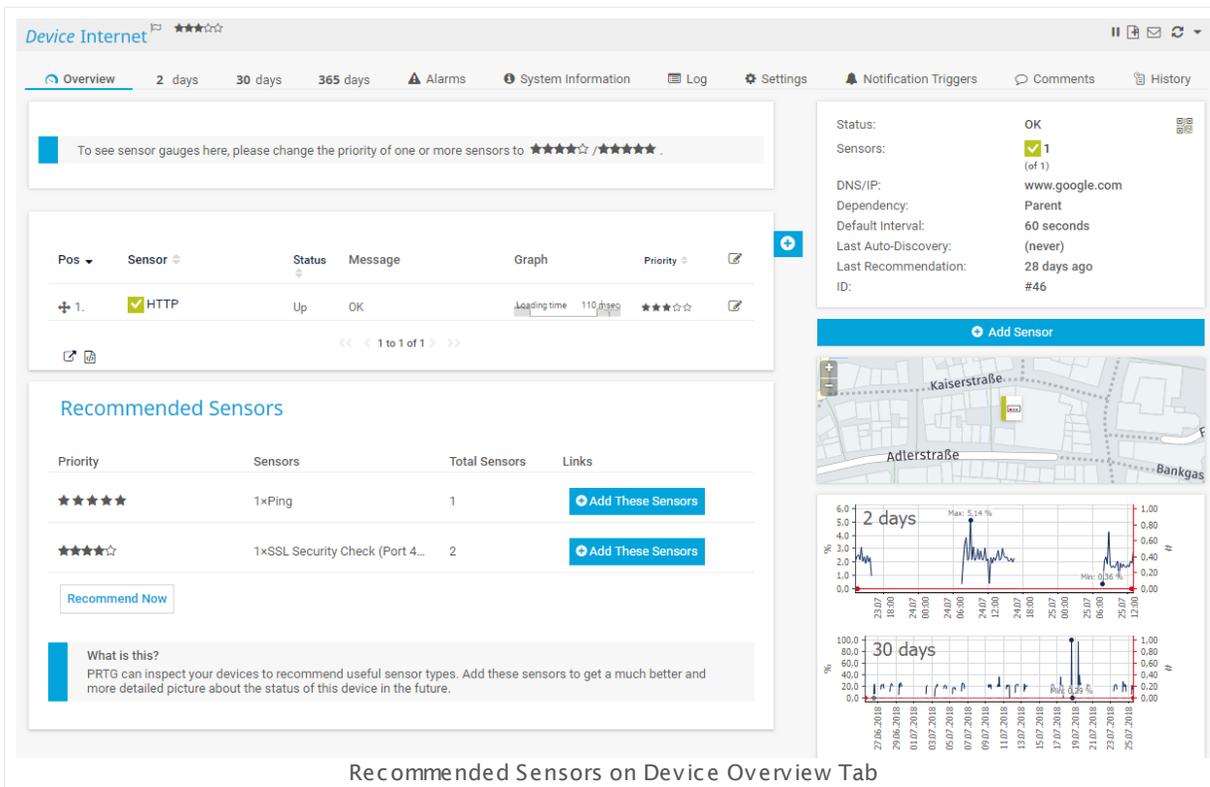
SIMILAR SENSORS FILTERS

Sensors Related To	Select the device, probe, or group that you want the similar sensors analysis to cover. This way, you can apply the analysis to the parts of your network that you are interested in.
With a Maximum Similarity of	Select a degree of similarity from 85 % to 100 %.
Inverted Relationships	<p>If you select Show, PRTG shows all similarity relationships, that is, A matches B and B matches A.</p> <p>If you select Hide, PRTG will show only A matches B relationships. This reduces the number of displayed similar sensors.</p>

6.9 Recommended Sensors

The **Recommended Sensors** function is one of the options that PRTG supports you in setting up a comprehensive monitoring. PRTG can explore any device and check which sensors you have already created. If it finds useful sensors that can [complete your monitoring](#)^[198] and are not yet created, you will find a list of recommended sensors for your specific device. By adding these sensors, you will not miss important monitoring data anymore!

 You cannot use this feature on the **Hosted Probe** of a PRTG hosted by Paessler instance. You can use this feature on [remote probes](#)^[370].



Recommended Sensors on Device Overview Tab

Get Sensor Recommendations

You want to know which sensors can complete the monitoring of your devices? By default, PRTG recommends sensors for any device that you add to PRTG and shows the suggested sensor types for it on the **Overview** tab of the device, as long as your installation contains less than 5,000 sensors in total. All you have to do is click the **Add These Sensors** button to enhance your monitoring experience.

If you want to manually start the detection engine for sensor recommendations on any desired device, follow the steps below.

You can see the [time passed since the last execution of the sensor recommendation in the page header bar](#)^[185] on the **Overview** tab of this device.

Step 1: Choose the Device

Open the [Overview](#)^[198] tab of the device that you want to analyze.

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Step 2: Recommend Now

To start the analysis of your device, click the **Recommend Now** button or choose the option **Recommend Now** in the [context menu](#)^[254].

i If you do not see the **Recommend Now** option, make sure that the sensor recommendation is enabled in the [System Administration—Monitoring](#)^[3359] settings. Probe devices do not offer this option.

Depending on the complexity of your device, it can take some time until you see the results of the analysis. Stay tuned!

Recommended Sensors



PRTG has started searching for sensors it can recommend for this device. You can see the search progress in the **Recommended Sensors** table. Please click **OK** to close this window.

OK

Recommended Sensors Investigation

PRTG runs the device analysis in the background with low priority to prevent potential performance issues. Consequently, the recommended sensors analysis can take more time than expected if PRTG needs resources to ensure gapless monitoring of your network in the first place. By default, the sensor recommendation engine starts automatically when you add a new device, when you do not have more than 5,000 sensors, or when the last analysis was executed more than 30 days ago. You can change these settings in the [System Administration—Monitoring](#)^[3359].

i To recommend [SNMP sensors](#)^[431] for a device, the detection engine uses the SNMP version that you defined in the [Credentials for SNMP Devices](#)^[411] section of the device settings.

Step 3: Get the Results

After analyzing your device, PRTG suggests a list of sensors that are useful for a more comprehensive monitoring.

Recommended Sensors

Priority	Sensors	Total Sensors	Links
★★★★★	1xPING	1	Add These Sensors
★★★★☆	1xSSL Security Check (Port 443), 1xSSL Certificate Sensor (Port ...	2	Add These Sensors

[Recommend Now](#)

What is this?
 PRTG can inspect your devices to recommend useful sensor types. Add these sensors to get a much better and more detailed picture about the status of this device in the future.

List of Recommended Sensors

The list of recommended sensors provides the following information:

RECOMMENDED SENSORS

Priority	Shows which priority ^[242] the suggested sensors will have when you add them. The recommended sensors table is sorted by priority, beginning with top priority (5***** stars) in the first row. ⓘ You can manually change the priority of a sensor after adding it.
Sensors	Shows the suggested sensors and the number of sensors from one type PRTG recommends for this device (for example, you might want to add a sensor from the type SNMP Traffic ^[240] multiple times because of several network interfaces).
Total Sensors	Shows the total number of suggested sensors per table row. These sensors have the same priority.
Links	Displays an Add These Sensors button for every table row. Click to automatically add the sensors listed in this table row to the device.

ⓘ The detection engine checks if a certain sensor type currently exists on your device and recommends that you add this sensor if it does not exist. If this sensor type already existed previously on the device but you have deleted it, PRTG will suggest this sensor type again. Please ignore the suggestion of this sensor type or follow [Step 4](#)^[215].

Step 4: Add Recommended Sensors

Click the **Add These Sensors** button in a table row to add all sensors in this row to the analyzed device.

i If you want to add **all** suggested sensors regardless of their priority, click every **Add These Sensors** button in the recommended sensors table. If you want to add only **some** of the sensors of a certain priority and not all of them, please click **Add These Sensors** first and then [delete](#)^[259] or [pause](#)^[245] the ones you do not need.

Settings for the Recommended Sensors Analysis

You can also adjust the recommended sensors detection. Go to [System Administration—Monitoring](#)^[339] to select whether

- you want PRTG to decide on the sensor recommendation (default), or
- you want the recommended sensors to always be displayed, or
- you want to turn off the recommended sensors function.

If you use the default setting, PRTG uses an intelligent assistant that takes care of your specific network monitoring situation. PRTG automatically counts the number of sensors you have and decides whether to start the recommended sensors detection or not. It will not start if your PRTG installation comprises 5,000 sensors or more to prevent performance issues. We recommend that you set this default option so you do not miss any important monitoring data about your network, without risking running into performance issues.

i Disable the recommended sensors feature if you encounter performance issues or if you do not want to display this information on device overview tabs.

More

Do you want to get more help with choosing and creating useful sensors? This is possible in PRTG with the [Auto-Discovery](#)^[282]. You can activate it when [adding a new device](#)^[313] to PRTG, [manually at any time](#)^[283], or choose if you want PRTG to [analyze a whole section](#)^[285] of your network, for example, devices covered by a certain IP range.

i The auto-discovery has a higher priority than the recommended sensors detection. If both are active, PRTG will queue the sensor recommendation and execute the auto-discovery first.

6.10 Object Settings

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Device Tree Management

The **Management** tab is available when viewing probes or groups. After clicking this tab you can move devices and sensors directly in the tree view. If moving is not possible, the web interface will automatically start a clone process.

 For more information, see the [Manage Device Tree](#) ³²⁹ section.

General Settings

In the **Settings** tab you can define all settings for the current object. The available options vary, depending on the kind of object you're changing. See the following sections for information about the respective object types:

- [Root Group Settings](#) ³³¹
- [Probe Settings](#) ³⁵¹
- [Group Settings](#) ³⁷⁵
- [Device Settings](#) ⁴⁰²
- [Sensor Settings](#) ⁴²⁸

 The available setting options are different for **each** sensor, but always the same for probes, groups, and devices. [Sensor Channels Settings](#) ³¹⁶⁰ are not reachable via tab but directly on a sensor's overview page via channel gauges and the channels table.

Notification Triggers Settings

In the **Notification Triggers** tab, notification triggers can be set for every object. When using these settings for a probe, group, or device, they will be inherited to all sensors on these objects. Available notification trigger options are the same for all objects.

 For more information, see [Sensor Notification Triggers Settings](#) ³¹⁷⁰ section.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

i On some pages, you can access the history of subordinate objects via the corresponding context button in the [page header bar](#)¹⁸⁵. This includes [System Administration](#)³³⁴³ and the overview pages of [User Accounts](#)³³⁷⁶, [User Groups](#)³³⁸³, [Reports](#)³²⁵², [Libraries](#)³²³⁵, and [Maps](#)³²⁷⁸. See the [Logs \(Main Menu\)](#)²²⁹ for details.

Related Topics

- [General Layout](#)¹⁸¹
- [Review Monitoring Data](#)¹⁹⁸
- [Toplists](#)³¹⁸⁶

6.11 Alarms

The alarms list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful for keeping track of all irregularities in your network.

In the [table list](#)²³⁷, you can re-sort the items by clicking the column's header items.

Sensors With Alarms Items: ~ 50
Show Filters

Sensor	Probe Group Device	Status	Down for	Last Value	Message	Graph	Priority
!! PING		Down	14 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	14 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	16 h 49 m		Request timed out (ICMP error # ...	Ping Time No data	★★★★★
!! PING		Down	14 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	20 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	14 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	8 d 19 h		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	6 d 16 h 57 m		Request timed out (ICMP error # ...	Ping Time No data	★★★★★
!! PING		Down	20 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	14 d		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	6 d 17 h 58 m		Request timed out (ICMP error # ...	Ping Time No data	★★★★★
!! PING		Down	16 h 51 m		Request timed out (ICMP error # ...	Ping Time No data	★★★★★
!! PING		Down	16 h 50 m		Host not found. This message in...	Ping Time No data	★★★★★
!! PING		Down	56 m 44 s		Request timed out (ICMP error # ...	Ping Time No data	★★★★★

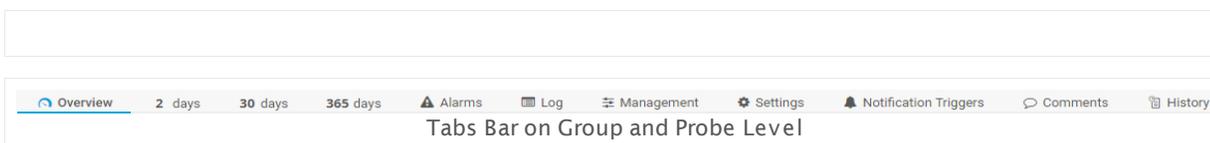
Alarms List

There are two ways to display the alarms list: either click the **Alarms** tab on the detail page of a probe, group, or device (not available for sensors), or click **Alarms** in the [main menu bar](#)²⁶³.

i By default, table lists with alarms are ordered by [priority](#)²⁴².

Alarms (Object Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



On an object's detail view, click the **Alarms** tab to show a table list of all sensors **on this object** that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. You will see a subset of sensors in an alarm status for the current object only. This is a subset of the entries available via the **Alarms | All** option in the [main menu bar](#)^[270]. The tab is not available on a sensor's detail page.

Alarms (Main Menu)

Click **Alarms** in the [main menu bar](#)^[270] to show a table list of **all** sensors in your configuration that currently show a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. You can also show these sensors as gauges. Click **Alarms** in the [main menu bar](#)^[263] and select another option to only show a subset of sensors in certain states. Choose between:

ALARMS	
All	Open a list of all sensors that are currently in Down , Down (Partial) , Down (Acknowledged) , Warning , or Unusual status ^[195] .
Show as Gauges	Open a page with the gauges of all sensors that are currently in Down , Down (Partial) , Down (Acknowledged) , Warning , or Unusual status. The size of the sensor gauges corresponds to their respective priority.
Errors Only	Open a list of all sensors that are currently in Down , Down (Partial) , or Down (Acknowledged) status.
Warnings Only	Open a list of all sensors that are currently in Warning status.
Unusuals Only	Open a list of all sensors that are currently in Unusual status.

Acknowledge Alarm

An acknowledged alarm shows up in the alarms list as "acknowledged" (see [Sensor States](#)^[195]) and will not [trigger](#)^[3170] any more [notifications](#)^[3216].

 If the alarm condition clears, the sensor usually returns to an **Up** status immediately with the next sensor scan.

To acknowledge an alarm, right-click a sensor entry and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the last message value of the sensor. You can choose between: **Acknowledge Indefinitely...**, **acknowledge For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**

If you choose **Until...** a dialog box appears:

ACKNOWLEDGE ALARM UNTIL

Selected Objects	Shows the sensor(s) that you want to acknowledge the alarm for. You can acknowledge alarms for more than one sensor using multi-edit ³¹⁹⁷ .
Message	Enter a text, for example, the reason why you acknowledge the alarm. Please enter a string or leave the field empty.
Until	Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time.  If the alarm condition still persists after the specified date, the sensor will show a Down status again.

Only [users](#)³³⁷⁶ with write access rights may acknowledge alarms. You can give read-only users the right to acknowledge alarms, too. See section [User Accounts Settings](#)³³⁷⁷, section **Account Control**.

More

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <https://kb.paessler.com/en/topic/26303>

6.12 System Information

The **System Information** is a great feature to see at a glance what is going on on the systems you have in your network. You get

- basic system data of your device like bios serial number or MAC and IP addresses,
- all connected hardware types as well as their states and properties,
- the software you have installed, including version and vendor information,
- the users connected to your system and their domain,
- a list of all active or stopped Windows system services plus their properties, and
- a list of all processes running on your system, including their ID and start time.

Together with your everyday monitoring you will receive a really profound knowledge about your IT infrastructure from only one single source—your PRTG Network Monitor!

The screenshot shows the 'System Information' tab for a device named 'Device Probe Device'. The navigation bar includes 'Overview', '2 days', '30 days', '365 days', 'Alarms', 'System Information' (selected), 'Log', 'Settings', 'Notification Triggers', 'Comments', and 'History'. The main content area is titled 'System Information' and has a blue header with expandable sections: System, Hardware, Software, Users, Services, and Processes. Below this, there are two panels: 'System' (updated 22 h 52 m ago) and 'Hardware' (updated 22 h 52 m ago). The 'System' panel shows a table with columns 'Name' and 'Value', listing items like 'Bios Serial Number', 'IPAddress / Intel(R) 82574L Gigabit Network Connection', and 'Windows Version'. The 'Hardware' panel shows a table with columns 'Name', 'Class', 'Caption', and 'Properties', listing items like '\\.\PHYSICALDRIVE0 (Disk dr...', 'Intel(R) 82574L Gigabit Netw...', 'Intel(R) Xeon(R) CPU E5-2680...', 'Microsoft ISATAP Adapter', 'Microsoft Kernel Debug Netw...', 'Microsoft XPS Document Wri...', 'Physical Memory', and 'Physical Memory Array'.

System Information Tab on a Windows Device

System Information is available for all devices that you add to PRTG and run with an [officially supported Windows version](#)^[26]. You can also retrieve system information from Linux, Unix, or other devices that have Simple Network Management Protocol (SNMP) enabled.

i Some of the above listed system information may not be available depending on the request method you use (Windows Management Instrumentation (WMI) or Simple Network Management Protocol (SNMP)). To get all information available, activate both request methods (Windows Management Instrumentation (WMI) **and** Simple Network Management Protocol (SNMP)), as far as possible.

Find and Use System Information

Go to the overview page of a device and click the **System Information** tab to see available information.

Basically, it is not necessary to configure anything special to use the **System Information** feature, if you already monitor a network device with [WMI](#)^[433] and [SNMP sensors](#)^[431]. The **PRTG System Information** uses the same [technologies](#)^[3488]. So, you already meet the main prerequisites for retrieving system information for your device. The data will be displayed in the corresponding **System Information** table automatically and you can [analyze your system directly](#)^[225]. If you are not using Windows Management Instrumentation (WMI) or Simple Network Management Protocol (SNMP) sensors yet, see section [Prerequisites](#)^[223] below that shows in detail what you need to get system information.

 **System Information** is enabled by default. To retrieve the data, PRTG will automatically use **Credentials for Windows Systems** and **Credentials for SNMP Devices** as defined in the [device settings](#)^[402] or as [inherited](#)^[133] from a parent object like the **Root** group. Please consider this when you monitor devices outside the local network, especially when using **SNMP v1** or **v2c** that do not provide encryption.

 System Information is not supported by the [Enterprise Console](#)^[3430]. Please use the [PRTG web interface](#)^[166] to access the system information of a device.

 System Information for your devices only has informational purposes. We cannot guarantee that the data displayed in PRTG Network Monitor fully corresponds to the device parameters.

 You cannot use this feature on the **Hosted Probe** of a PRTG hosted by Paessler instance. You can use this feature on [remote probes](#)^[3709].

Prerequisites

Fulfill the following requirements to show all available system information data for a device. It is not necessary to meet every single prerequisite but then some tables will not show all data or may even remain empty. For example, if you do not configure SNMP on the target device, you will get less information for the **System** table.

- **Valid credentials** in the [device settings](#)^[402] (or [inherited](#)^[133]): Enter correct settings for the target device in the sections **Credentials for Windows Systems** and **Credentials for SNMP Devices**.
- **Remote Registry** Windows service: Enable the **Remote Registry** Windows service on the target computer, for example, via **services.msc**, and set the start type to **automatic**.
- **Remote Procedure Call (RPC)** Windows service: Enable the RPC Windows service on the target computer, for example, via **services.msc**, and set the start type to **automatic**.
- **WMI** on probe and target computer: Configure Windows Management Instrumentation (WMI) on the target computer and on the computer that runs the PRTG probe with the device. Especially configure the firewall of the target computer to allow WMI. For more details, see manual section [Monitoring via WMI](#)^[3507] and the Knowledge Base article [General Introduction to WMI and PRTG](#).

- **SNMP** on target computer: Configure Simple Network Management Protocol (SNMP) on the target computer. For more details, see manual section [Monitoring via SNMP](#)^[3489] and the Knowledge Base article [General Introduction to SNMP and PRTG](#).

Usually you will see data coming in after a few minutes, depending on the protocols you use (WMI takes longer than SNMP). A **System Information** table will show an error message, if PRTG cannot get data, for example, because of misconfiguration.

- For details about error messages, see this Knowledge Base article: [How can PRTG get data for System Information tables?](#)

Software
31 5 Ago



No Data Available

- *Error: Could not connect to the remote registry service of the target system. Make sure the service is running and the Windows credentials are correct. (code: PE255)*
- *Error: Could not connect to the remote registry service of the target system. Make sure the service is running and the Windows credentials are correct. (code: PE255)*
- *Error: SNMP No Response*

No Data Available: Check the Preconditions

System Information (Device Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.

Overview
2 days
30 days
365 days
Alarms
System Information
Log
Settings
Notifications
Comments
History

Tabs Bar on Device Level

On the details page of a device, click the **System Information** tab.

- If you do not see a **System Information** tab for your device, you need to enable **System Information** in section [Advanced Network Monitoring](#)^[425] in the device settings (or inherit it from an object higher in the [hierarchy](#)^[133]). **System Information** is enabled by default. If **System information** is disabled, the **System Information** tab will not be available for the device.

Analyze Your Systems

On the **System Information** page, PRTG displays a table for each system information category about this device: **System**, **Hardware**, **Software**, **Users**, **Services**, and **Processes**.

CATEGORY	SYSTEM INFORMATION	REQUEST METHOD
System	Shows information about the device like BIOS serial number, IP addresses, MAC addresses, and Windows version.	 WMI  SNMP
Hardware	Shows hardware that is connected to the device like disk drives, CD/DVD, video controllers, processors, network adapters, sound devices, printers, and memory. You can see Class and Caption of a hardware device. In the Properties column you get more information about the hardware (for example, the description).	 WMI  SNMP
Software	<p>Shows installed software and the Version number on the device. In the Properties column you get more information about the software (for example, the size).</p> <p> PRTG uses Uninstall registry keys to retrieve the list of installed software, so the displayed software might differ from the software that the target Windows system shows under Programs and Features.</p> <p> The System Information scan for software on the probe device uses the credentials the probe¹²⁶ runs with and ignores credentials from the Settings tab.</p>	 WMI  SNMP
Users	Shows the user accounts connected to the device and their Domain .	 WMI  SNMP
Services	Shows the available Windows services on the device. This table shows the State of the service (running, stopped) and the start type (Start mode automatic, manual, or disabled). In the Properties column you can get more information about a service (for example, the description).	 WMI  SNMP
Processes	Shows the processes that are currently running on the device as listed on the Processes tab of the Windows Task Manager. You can also see the Start Time (only WMI) and Process ID of a process.	 WMI  SNMP

Click the refresh button in the upper-right corner of a table to retrieve current information for this **System Information** category. The timestamp shows the time passed since the last table refresh.

31 S Ago 
Table Refresh

PRTG automatically retrieves data for all tables, including **System**, **Hardware**, and **Software**, once every 24 hours. The tables **Users**, **Services**, and **Processes** refresh each time you open the **System Information** tab. PRTG also updates all system information tables when the PRTG server is restarted, for example, after an update.

-  PRTG can perform up to 24 system information scans simultaneously so it may take some time until the tables are filled after a server restart.
-  You can sort each table by clicking the column headers. See [Working with Table Lists](#) ²³⁷ section for more information.
-  PRTG user accounts with read-only [access rights](#) ¹⁵⁸ to a device can view system information on this device but they cannot refresh tables manually.

Data Storage

PRTG stores data files with the retrieved system information in the corresponding **\System Information Database** subfolder of the [PRTG data folder](#) ³⁷³⁴.

-  If you delete a device in PRTG, the system information files of this device will remain in these folders unless you delete them manually.

PRTG uses the following subfolders for **System Information** data.

SYSTEM INFORMATION DATABASE: DATA FOLDERS

hardware	Data for the Hardware table
loggedonusers	Data for the Users table
processes	Data for the Processes table
services	Data for the Services table
software	Data for the Software table
system	Data for the System table

More

Knowledge Base: How can PRTG get data for System Information tables?

- <https://kb.paessler.com/en/topic/67824>

Knowledge Base: General Introduction to WMI and PRTG

- <https://kb.paessler.com/en/topic/1043>

Knowledge Base: General Introduction to SNMP and PRTG

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why do I get DoS Alarms on my QNAP?

- <https://kb.paessler.com/en/topic/80421>

6.13 Logs

Logs show all past activities and events of your PRTG monitoring setup. This is useful for researching past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of log data is produced. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

There are several filters available to make navigating the log entries easier. See the [Working with Table Lists](#) section for more information.

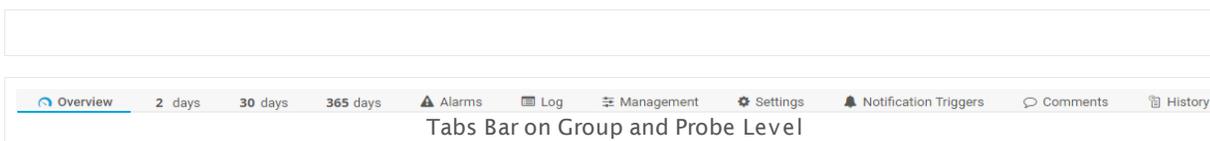
Log Entries Items: ~ 50
Show Filters

Date Time	Parent	Type	Object	Status	Message
8/8/2017 9:22:32 AM	None	Web Server Options		Edited	See history for details.
8/8/2017 9:11:02 AM	Sharepoint 01	PerfCounter IIS Application P...	App Pool .NET v4.5 Classic	Up	Running
8/8/2017 9:11:02 AM	Sharepoint 01	PerfCounter IIS Application P...	App Pool .NET v4.5 Classic	Warning	Range check error
8/8/2017 9:04:02 AM	WINDOWS	Device	DomainController	Edited	See history for details.
8/8/2017 9:01:06 AM	None	Group	Root	Notification Info	Report Email "[PRTG Network ...
8/8/2017 8:57:50 AM	Probe Device	Business Process	Business Process 1	Edited	See history for details.
8/8/2017 8:55:59 AM	None	PRTG (Administrator)	PRTG System Administrator	Edited	See history for details.
8/8/2017 8:52:45 AM	ServerSimulation	WMI Vital System Data (V2)	Server: Bytes Received/sec	Down	Range check error
8/8/2017 8:48:52 AM	None	PRTG (Administrator)	PRTG System Administrator	Edited	See history for details.
8/8/2017 8:37:45 AM	ServerSimulation	WMI Vital System Data (V2)	Server: Bytes Received/sec	Warning	Range check error
8/8/2017 8:37:01 AM	CBQoS	SNMP Cisco CBQoS	CBQoS Match ip dscp ef (46) (Main Interface:1 ...	Unknown	No data since 8/8/2017 7:50:5...
8/8/2017 8:08:00 AM	Probe Device	QoS (Quality of Service) Roun...	QoS (Quality of Service) Round Trip	Unknown	No data since 8/8/2017 8:06:1...
8/8/2017 8:07:26 AM	Probe Device	QoS (Quality of Service) One ...	QoS (Quality of Service) One Way	Down	Timeout. No packets received. ...
8/8/2017 8:07:01 AM	Probe Device	QoS (Quality of Service) One ...	QoS (Quality of Service) One Way	Unknown	No data since 8/8/2017 8:03:2...
8/8/2017 8:05:13 AM	Local Probe	Device	Probe Device	Edited	See history for details.
8/8/2017 8:05:09 AM	Local Probe	Device	Probe Device	Edited	See history for details.
8/8/2017 8:00:47 AM	None	Group	Root	Notification Info	Report Email "[PRTG Network ...
8/8/2017 7:01:02 AM	None	Group	Root	Notification Info	Report Email "[PRTG Network ...
8/8/2017 6:01:01 AM	None	Group	Root	Notification Info	Report Email "[PRTG Network ...
8/8/2017 5:09:29 AM	Probe Device	QoS (Quality of Service) Roun...	QoS (Quality of Service) Round Trip	Down	Access violation at address 00...
8/8/2017 5:09:09 AM	Probe Device	QoS (Quality of Service) Roun...	QoS (Quality of Service) Round Trip	Warning	Access violation at address 00...
8/8/2017 5:09:00 AM	Probe Device	QoS (Quality of Service) Roun...	QoS (Quality of Service) Round Trip	Up	4 msec

List with Log Entries

There are two options to open the logs list: Either you click the **Log** tab on the detail page of a probe, group, device, or sensor, or you choose the **Logs** item in the main menu.

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.



Click the **Log** tab to show a table list with all log information **on this object**. This is a more detailed log than the system log available via the **Logs | All** option in [main menu](#)^[273].

Logs (Main Menu)

Click **Logs** in the [main menu bar](#)^[273] to show a table list of all system log entries in your configuration. **Hover** over **Logs** and select another option to narrow down your log search. Choose between:

LOGS	
All	Open a table list ^[237] with log information for all objects in your configuration, newest first.
Status Changes >	Open a list with log information for certain status changes only. Hover over Status Changes to show other menu items. Follow the menu path to view log entries with a special value in the Status field only. Select between Up & Down (shows entries with either Up or Down in the Status field), Down, Warning, Unusual, Up, Paused/Resumed (shows entries with either Paused or Resumed in the Status field), or Acknowledged Alarms .
System Events >	Open a list with log information regarding certain system event types only. Hover over System Events to show other menu items. Select between the following event types: Probe Related, Cluster Related, Auto-Discovery, Notifications, or Status Messages .
Object History	<p>Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The object history page has a tab-like interface. Using the tabs you can navigate through various sub-pages in order to view the changes to all related settings and deletions of objects. Select between the following tabs: My Account, System Administration, Notifications, Schedules, User Accounts, User Groups, Reports, Libraries, or Maps.</p> <p> You can open a specific tab directly with the context button History in the page header bar^[185] on the corresponding pages.</p>

More

Knowledge Base: The logs page in the PRTG web interface does not load. What can I do?

- <https://kb.paessler.com/en/topic/77329>

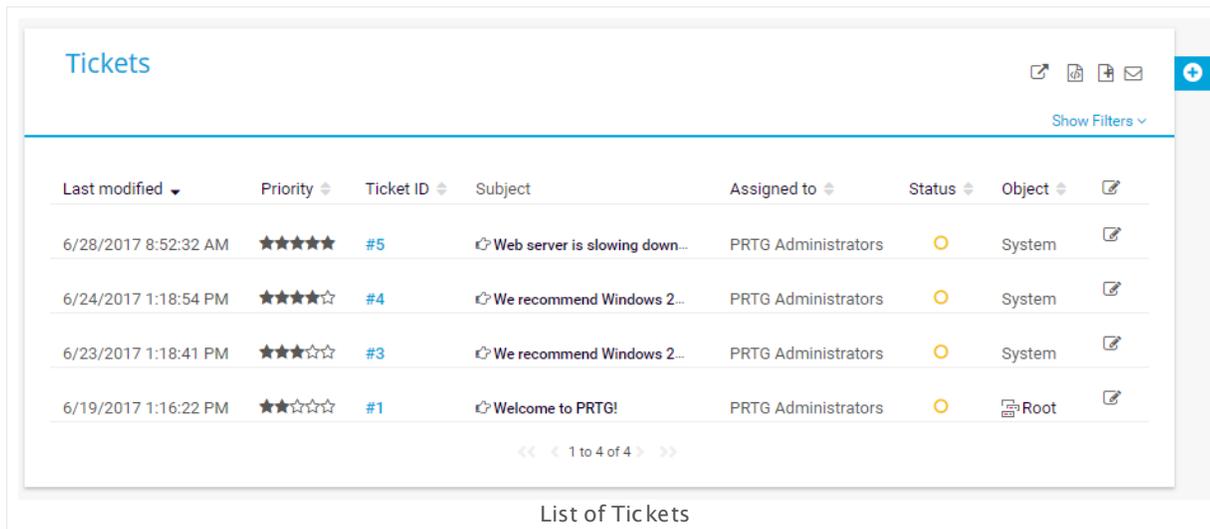
6.14 Tickets

PRTG Network Monitor includes its own ticket system. With tickets you can manage and maintain various issues that may appear while monitoring a network. A ticket in PRTG contains information about recent events in your PRTG installation that need a closer look by the administrator or another responsible person. You can see each ticket as a task for a particular PRTG user.

Each monitoring related task has a lifecycle in the ticket system. PRTG itself can create tickets, for example, when [Auto-Discovery](#)^[282] has finished, and PRTG users can create tickets as well for every kind of issue. In addition, you can set up notifications that open a ticket when something uncommon occurs in your network. The task comes to life when a ticket is created. Responsible PRTG users then take care of this issue. Once the issue has been resolved, the ticket can be closed and the lifecycle of the task ends.

Every ticket has a unique ID, a priority, and a status, and you can take several actions on each ticket. You should view every ticket and take a corresponding action. This way, you always keep an overview about each task and its history in your PRTG installation.

PRTG can also send an email to you whenever a ticket is assigned to you or if one of your tickets has been changed. See section [Tickets as Emails](#)^[234] for details and how to turn off emails about tickets.



Last modified	Priority	Ticket ID	Subject	Assigned to	Status	Object	
6/28/2017 8:52:32 AM	★★★★★	#5	Web server is slowing down...	PRTG Administrators	○	System	✎
6/24/2017 1:18:54 PM	★★★★☆	#4	We recommend Windows 2...	PRTG Administrators	○	System	✎
6/23/2017 1:18:41 PM	★★★☆☆	#3	We recommend Windows 2...	PRTG Administrators	○	System	✎
6/19/2017 1:16:22 PM	★★☆☆☆	#1	Welcome to PRTG!	PRTG Administrators	○	Root	✎

List of Tickets

i You can turn off the tickets system for particular user groups in [System Administration—User Groups](#)^[3383] except for the PRTG Administrators group. The users in the admin group will not receive new ToDo tickets (and notifications about changes) by default, only the PRTG System Administrator user. You cannot change this behavior. However, you can [turn off ticket emails](#)^[234] for every user account.

Types of Tickets

New tickets are created in the following cases:

- New devices or sensors have been created by the auto-discovery process.
 - ❗ In the corresponding ticket, only device templates will be listed that PRTG used to create sensors.
- A new probe connects to the core and must be acknowledged.
- A new cluster node connects to the cluster and must be acknowledged.
- A new version of the software is available.
- A new report is ready for review.
- In a few other situations, such as when the system runs out of disk space, for licensing issues, when an error occurs, etc.
- A [notification](#)  opened a ticket if set in the notification settings.
- A user opened a ticket.

Overall, there are three types of tickets:

- **User Tickets:** Tickets created by PRTG users, for example, to assign monitoring related tasks to a particular PRTG user (or user group)
- **ToDo Tickets:** Tickets created by PRTG to show important system information and in case of specific system events. They are assigned to the PRTG System Administrator user and cannot be turned off.
 - ❗ The **Related Object** of ToDo tickets is **System**.
- **Notification Tickets:** Tickets created via [Notifications](#)  in case of monitoring alerts

States of Tickets

Tickets can have three different states depending on the working process regarding the corresponding issue:

Sym bol	State	Description
	Open	New tickets will be open as long as the corresponding issue exists as described in the ticket.
	Resolved	The issue as described in the ticket does not persist any longer. Someone took care of it.
	Closed	Usually, the ticket has been resolved before, the solution to the issue has been checked for correctness, and the ticket does not require any other action.

Tickets (Main Menu)

 This option is only shown in the main menu bar if the user group of the current user is allowed to use the ticket system. You can turn off tickets for particular user groups in [System Administration—User Groups](#)³³⁸³. Users with **read-only** rights are always excluded from the ticket system and cannot see the tickets entry in the main menu bar.

You have several options to display a list of tickets that is filtered to your needs. In the [main menu bar](#)²⁶³, **hover** over **Tickets** to show all available filter options or **click** directly to show all open tickets assigned to the current user. You can also create a new ticket via the main menu. Available options are:

- **My Tickets**
Click to show all open tickets that are assigned to the current user. **Hover** over **My Tickets** show other menu items for filtering these tickets depending on their status:
 - **Open**
 - **Resolved**
 - **Closed**
 - **All**
- **All Tickets**
Click to show all open tickets of all PRTG users. **Hover** over **All Tickets** to show other menu items for filtering these tickets depending on their status:
 - **Open**
 - **Resolved**
 - **Closed**
 - **All**
- **ToDo Tickets**
Click to show all open tickets from the [type](#)²³⁰ **ToDo**. **Hover** over **ToDo Tickets** to show other menu items for filtering these tickets depending on their status:
 - **Open**
Click to show all open ToDo tickets. **Hover** over **Open** to show other menu items for filtering these tickets depending on their event type:
 - **Report Related**
 - **Auto-Discovery Related**
 - **Probe Related**
 - **System Errors**
 - **New Software Version**
 - **Resolved**
 - **Closed**

- **All**
- **Open Ticket**
 Hover over  and select **Add Ticket** from the menu. This will open the **Add Ticket** dialog. In the first step, select the object on which you want to focus in the ticket via the **Object Selector**^[240]. Click **OK**.
 You can leave this step out when using the **context menu**^[247] of this object in the device tree to open the ticket.

In step 2, provide the following information and confirm by clicking on **OK** to create a **User Ticket**:

- **Subject**: Enter a meaningful title for the ticket that indicates the topic of the issue.
- **Assigned to**: Select a user (or user group) who will be responsible for this issue from the dropdown list.
- **Priority**: Define a **priority**^[242] from one to five stars.
- **Comments**: Enter a text message. This message should describe the issue in detail.

After selecting the desired filter or opening a new user ticket, a corresponding list of tickets will appear. In this table list, you can re-sort the items by using the **respective options**^[237]. Additionally, you have several search options using the inline filter directly above the table. The following filters are available:

- **Ticket status**: all, open, resolved, closed
- **Ticket type**: User, ToDo, Notification
- **Concerned user(s)**: Show only tickets that are assigned to a specific user or user group. There are the following types:
 - **anyone**: no user filter is applied so all tickets on this PRTG server are shown
 - **me**: show tickets that are assigned to you (the user who is currently logged in)
 - **Groups**: show tickets that are assigned to a specific user group only
 - **Users**: show tickets that are assigned to a specific user only
 - **Disallowed**: users or user groups that do not have access rights to the selected object are displayed under **Disallowed**. This for your information only; you cannot select them!
- **Relationship to a monitoring object**: Choose groups, probes, devices, or sensors with the **Object Selector**^[240].
 ToDo tickets are related to **System**.
- **Time span** to view tickets by last edit of a ticket: Use the date time picker to enter the date and time.

Click on the subject of a ticket to open the ticket's detail page. There you can find all related information, as well as conduct several actions.

ToDo Ticket #68 ★☆☆☆☆ 📄 ✉

Software update is available

Status: open Assigned to: PRTG Administrators Related Object: System Type: ToDo (New Software Version) ID: #68 [✎ Edit](#) [👤 Assign](#) [✔ Resolve](#) [🗑 Close](#)

Last Update

Opened by PRTG System Administrator+ Assigned to PRTG Administrators 28.08.2017 08:44:34

[28.08.2017 08:44:34] Version 17.3.34.2739 has been downloaded and is ready for installation. Please visit Setup|Autoupdate to initiate the installation.

An Open ToDo Ticket with Instructions

Actions

For best experience with PRTG, check every ticket and select appropriate actions.

i Only members of user groups that have the corresponding [access rights](#)¹⁵⁹ can view and edit tickets that are related to a certain monitoring object.

The following actions are available when viewing the tickets list or a specific ticket:

- **Edit**: Opens a dialog where you can change the subject and the priority of the ticket, as well as assign the ticket to another user. Furthermore, you can add a text message to this ticket. Confirm your changes by clicking **OK**.
- **Assign**: Opens a dialog where you can give the ticket to another user. Select a user (or user group) via the dropdown menu. Furthermore, you can add a text message to this ticket. Confirm your assignment by clicking **Save**.
- **Resolve**: Opens a dialog where you can resolve the ticket by clicking **Save**. The status **resolved** indicates that the issue as described in this ticket does not persist. Furthermore, you can add a text message to this ticket that indicates, for example, what has been done concerning the issue.
- **Close**: Opens a dialog where you can close the ticket by clicking **Save**. Usually, this ticket has been resolved before and the correct solution of the issue has been checked. Furthermore, you can add a text message to this ticket.
- **Reopen**: Opens a dialog where you can reopen a ticket after it has been resolved or closed. Do so, for example, if the solution of the issue turned out to be incorrect. Furthermore, you can add a text message to this ticket that indicates, for example, why you have opened the ticket again. Confirm reopening and assignment by clicking **Save**.

Tickets as Emails

You can receive all tickets that are assigned to you or to your user group as emails. You will also be notified via email each time this ticket is edited. This way, you will always be informed about new notifications (if set), important system information (if PRTG System Administrator), or within the communication with other PRTG users. You can turn off the setting **Tickets as Emails** in [System Administration—User Accounts](#)³³⁷⁶. If you disable emails for tickets for a user account, this particular user will not receive any ticket emails anymore.

i If you have defined to get tickets as emails and you are PRTG System Administrator, you will receive emails for ToDo tickets as well, although ToDo tickets are considered to be opened by the PRTG System Administrator.

More

Paessler Blog: A New Feature Was Assigned to You in PRTG: Ticket System Keeps Track of Network Monitoring Issues

- <https://www.paessler.com/blog/2014/02/03/prtg/ticket-system-keeps-track-of-network-monitoring-issues>

Ajax Web Interface—Basic Procedures—Topics

- [Login](#)^[168]
- [SSL Certificate Warning](#)^[172]
- [Welcome Page](#)^[175]
 - [Customer Service](#)^[178]
- [General Layout](#)^[181]
- [Sensor States](#)^[195]
- [Review Monitoring Data](#)^[198]
- Compare Sensors
- [Historic Data Reports](#)^[204]
- [Similar Sensors](#)^[209]
- [Recommended Sensors](#)^[213]
- [Object Settings](#)^[217]
- [Alarms](#)^[219]
- [System Information](#)^[222]
- [Logs](#)^[228]
- [Tickets](#)^[230]
- [Working with Table Lists](#)^[237]
- [Object Selector](#)^[240]
- [Priority and Favorites](#)^[242]
- [Pause](#)^[245]
- [Context Menus](#)^[247]
- [Hover Popup](#)^[262]
- [Main Menu Structure](#)^[263]

Other Ajax Web Interface Sections

- [Ajax Web Interface—Device and Sensor Setup](#)  280
- [Ajax Web Interface—Advanced Procedures](#)  318

Related Topics

- [Enterprise Console](#)  343
- [PRTG Apps for Mobile Network Monitoring](#)  348

6.15 Working with Table Lists

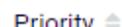
Throughout the web interface you often see table lists of items, for example, sensor or device lists. Table lists are also available on the overview pages of [Libraries](#), [Maps](#), [Reports](#), [Notifications](#), and [Schedules](#), as well as in [Logs](#) and [Tickets](#). All these provide common functionality. Depending on the type of content in the list, tables show various information in their columns for each object.

On certain overview pages, like for [sensors](#), [tickets](#), and [similar sensors](#), there is also an in-line filter available directly above the table. The filter options depend on the current page.

Ping Sensors Items: ~ 50
Show Filters v

Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	1 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	1 msec	OK		★★★★★	🔖	
✓ PING		Up	1 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	1 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	0 msec	OK		★★★★★	🔖	
✓ PING		Up	1 msec	OK		★★★★★	🔖	

Example of a Table List

FEATURE	DISPLAY	WHAT IT DOES
Paging		The content of a table is displayed over several pages. Click the arrow symbols at the end of a list to view other pages, or to jump to the beginning or the end of the list.
New Window		Click the window symbol at the beginning of a list to open the table in a new window.
Date Range		Use the date and time picker to show table list entries within a specific time span. Click the first date field for the start date and the second field for the end date. A calendar dialog opens where you can select date and time. Click the Done button to apply the selected date and time.
Select Range		When viewing log lists (not available in other lists), click Select Range in the upper-right corner of the list to select the time span you want to show log entries for. Choose between Today , Yesterday , and several other time spans. Choose Unlimited to disable this filter again.
Items		Click Items at the beginning of the list to select how many rows are shown on each page. Choose between 50 , 100 , 500 , and 1000 .
Sorting		Click the column headers to sort lists by the respective column. You select all words with arrows next to them for sorting, for example, by Status , Last Value , Priority , and more. The available options vary depending on the type of list.
Show XML		Click the XML option at the beginning of a list to download the current page in XML format. Your browser will usually show a download dialog.
Filtering		Use the filter options to show specific objects in the list. Enter one or more Tags into the field Tagged With to filter the list for corresponding objects. You can use the add (+) and remove (X) signs to categorize tags as "must have this tag" or "must not have this tag".

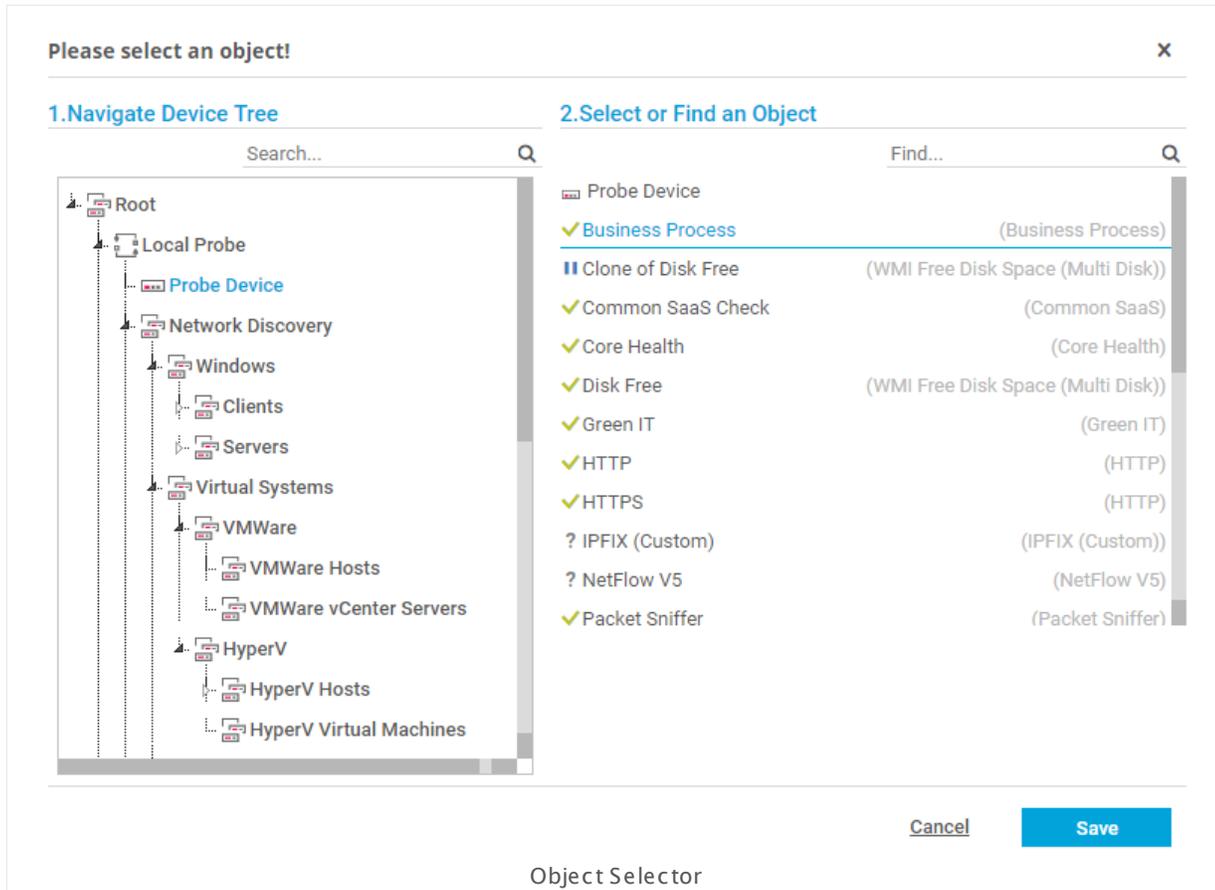
Click the entry below **Related to** to choose an object from the device tree with the **Object Selector** to show corresponding objects.

Related Topics

- [Multi-Edit Lists](#) 

6.16 Object Selector

For some functions, the object selector is shown. It enables you to browse all objects in your configuration and select an object in two steps.



Step 1: Navigate Device Tree

On the left-hand side, you see a device tree specific to your setup that you can browse by clicking the corresponding nodes. Click a device to view its sensors on the right-hand side.

You can directly browse for objects in the device tree by entering a probe name, group name, or device name into the **Search...** field above the device tree navigation. You can also use a substring only. The resulting objects will be displayed immediately without any manual confirmation.

Step 2: Select an Object

If you have selected a device on the left-hand side, you will see the sensors on this device here, on the right-hand side. Also, the sensor type is shown. **Hover** over a sensor on the right side to view its parent device and group.

You can also directly search and find sensors by entering the sensor name, group name, device name, or tag into the **Find...** box above the sensor list.

Select an object and click the **Save** button.

6.17 Priority and Favorites

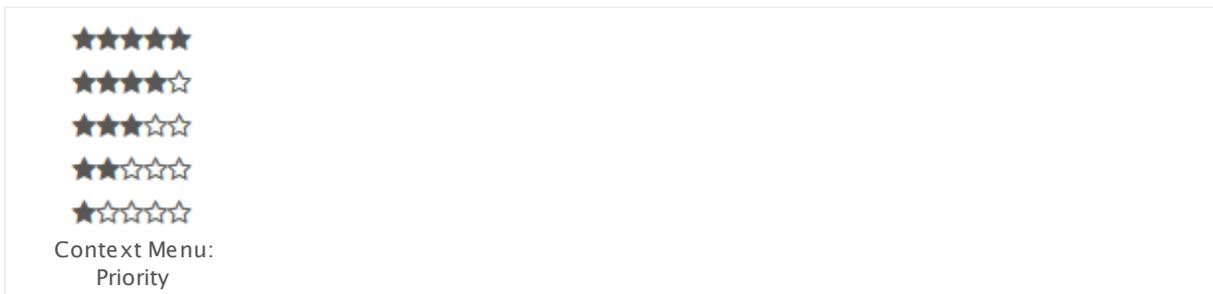
You can set priorities for all your monitoring objects and also categorize devices or sensors as favorites. Both settings affect how your objects are displayed.

- ⓘ Settings for priority and favorites are stored for the entire installation. They are not user specific.

Priority for All Objects

The priority setting affects the order in which your objects are displayed when you view table lists. PRTG lists objects with a higher priority first, others underneath, depending on their own priority. Furthermore, [device overview pages display gauges](#)^[198] for sensors with a high priority.

To change priority settings, **right-click** an object to open the [context menu](#)^[247] and select **Priority/Favorite**. You can choose between 5 stars ********* (top priority) and one star ***** (lowest priority). By default, all objects are set to medium priority (3 stars *****)**. In the page header bar and in lists, you can set a priority directly with one click on a star, for example, for sensors on a device overview page.

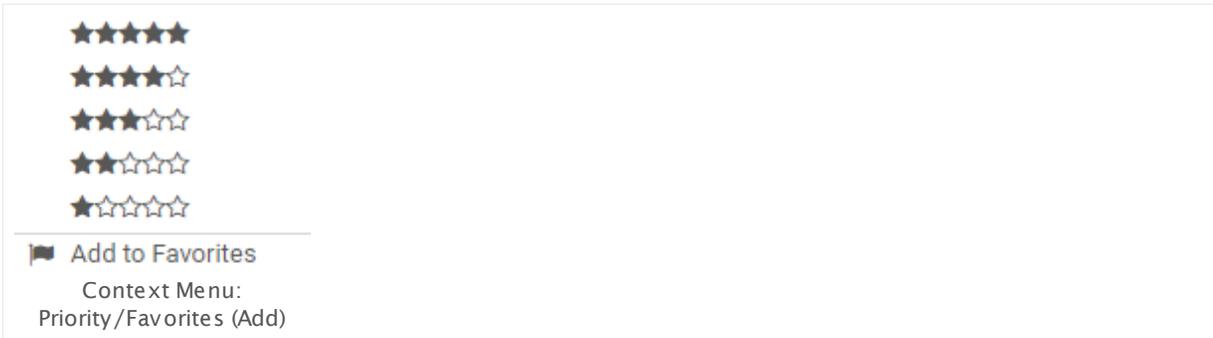


- ⓘ Select 4 or 5 stars for particular sensors to activate their gauges on device overview pages.
- ⓘ Select 5 stars for a map to show it as an entry in the [main menu bar](#)^[263] under **Home**.

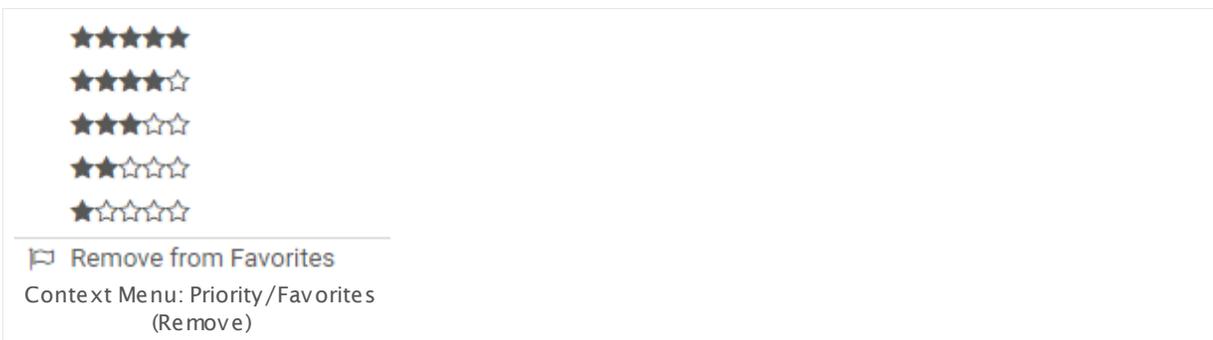
Favorites for Devices and Sensors

To call a list of all your favorite devices or sensors, select **Devices | Favorite Devices** or **Sensors | Favorite Sensors** from the main menu. These lists are sorted by priority as well.

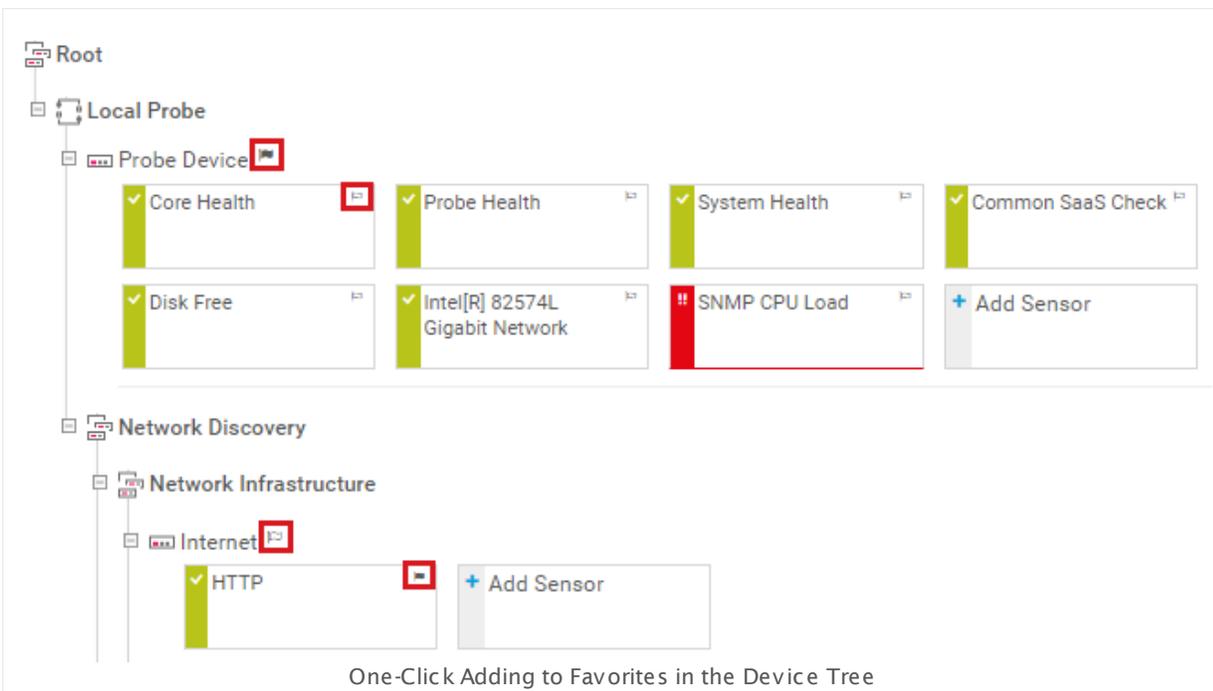
You can mark any device or sensor as favorite to add it to the favorite list. Right-click it to open the [context menu](#)^[247]. Select **Priority/Favorite | Add to Favorites**. A small black flag symbol will be added next to the object's name.



To remove an object from the favorites list, select **Priority/Favorite | Remove from Favorites** from the [context menu](#)^[247].

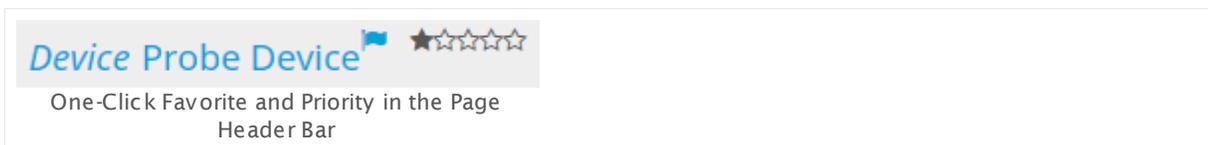


There is also the option to add a device or sensor to favorites with one click in the device tree. Just click the small flag symbol to the right of the respective object name. If the flag is black, the specific object is already a favorite; clicking the flag again will remove it from favorites and the flag will turn gray again.



Priority and Favorites in the Page Header Bar

You can add any device or sensor to favorites on its details page by clicking the small flag symbol in the [page header bar](#)¹⁸⁵. If the flag is blue, the selected object is already a favorite. Clicking the flag again will remove it from favorites and the flag will turn gray again. It is also possible to set the priority of the object by clicking one of the five stars in the page header; five stars ********* means top priority, one star ***** is the lowest priority.



6.18 Pause

If you want to pause monitoring, you have several possibilities to do so in PRTG. You can pause monitoring for a single sensor, an entire device, group, or even probe.

i While a sensor is paused, it will not collect any monitoring data, will not change its [status](#)^[195], and will not trigger any [notifications](#)^[143]. An object will keep its pause status also after a restart of PRTG.

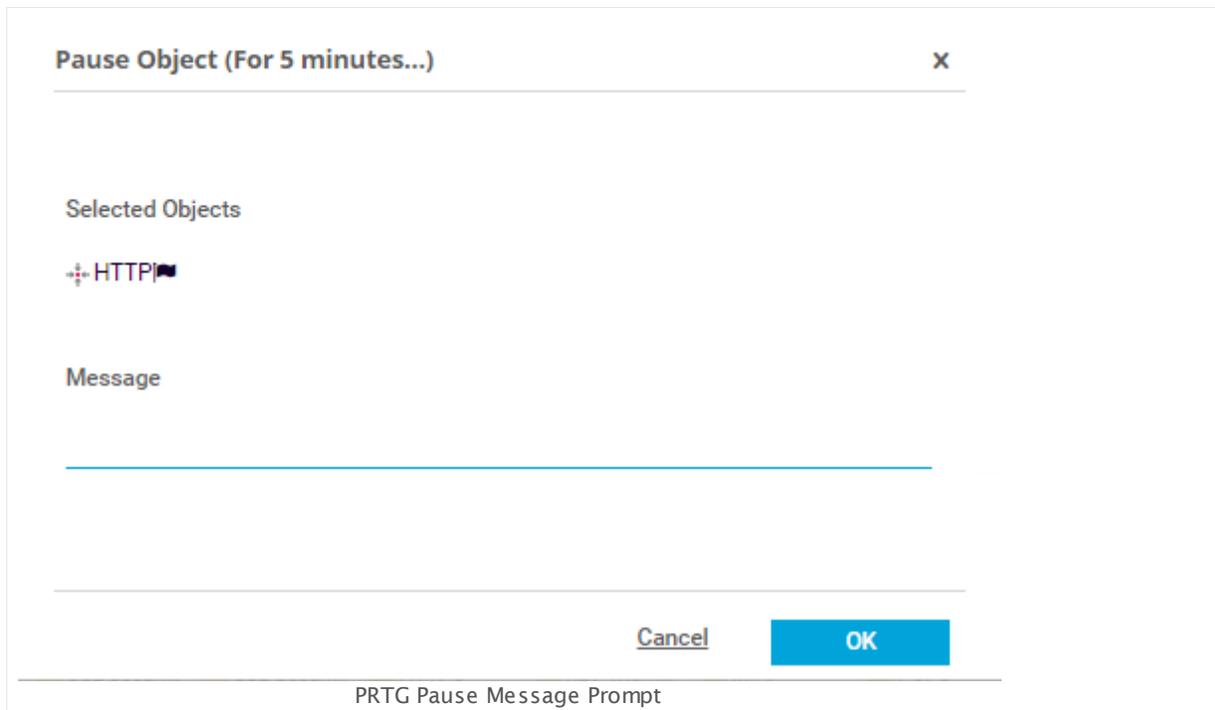
Pause by Intention—Manually or by Schedule

Navigate to the desired object in the device tree and select **Pause** from the [context menu](#)^[247].

You can choose **Pause Indefinitely**, or select a time after which monitoring will resume automatically, such as **5 or 15 minutes**, **1 or 3 hours**, **1 day**, or **Until** a certain date. You can also set up a one-time maintenance window to pause sensors automatically at a specified time.

i When selecting the **Pause** symbol from an object's [hover popup](#)^[262] or while using [multi-edit](#)^[3197], the object(s) will be paused indefinitely until resumed.

When selecting a pause option, you are prompted to enter a message. It will be shown in the status message of the object as long as it is paused. Confirm with **OK** to pause the object or click **Cancel** to not pause it.



The screenshot shows a dialog box titled "Pause Object (For 5 minutes...)" with a close button (X) in the top right corner. Below the title bar, there is a section labeled "Selected Objects" which contains a single entry: "HTTP" with a small icon to its left. Below this, there is a section labeled "Message" with a large, empty text input field. At the bottom of the dialog, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted in blue. Below the dialog box, the text "PRTG Pause Message Prompt" is visible.

i Monitoring for objects can also be paused by applying a schedule (see [Account Settings —Schedules](#)^[3338]) in the [Object Settings](#)^[217]. If you pause a master object by schedule or manually, you do not trigger a status change by [dependency](#)^[141]. See this Knowledge Base article [Why will dependent objects not go into paused status automatically when I pause the master object?](#)

Pause by Hierarchy

If you pause monitoring for a given object in the [device tree](#)^[181], all child objects underneath will be paused as well. For example, if you pause a group, all sensors on all devices in this group will also be paused. Once an object is paused, you can resume monitoring at any time by selecting **Resume** from the [context menu](#)^[247]. However, you cannot resume monitoring for single child objects that are paused by a parent object, only for the object you originally set to pause.

Pause by Dependency

There is a way you can make PRTG pause objects automatically. If you have a master object, for example, a master Ping sensor for a device, PRTG can pause all dependent sensors on the device automatically in case the master object is down. See [Dependencies](#)^[141] for more information and mind this Knowledge Base article [Why will dependent objects not go into paused status automatically when I pause the master object?](#)

6.19 Context Menus

Right-click on an object to view a context menu with many options for direct access to monitoring data and functions. You can also access many of the functionalities via the [main menu](#)^[263] or the [hover popup](#)^[262] window. However, using the context menu is the easier way in most cases.

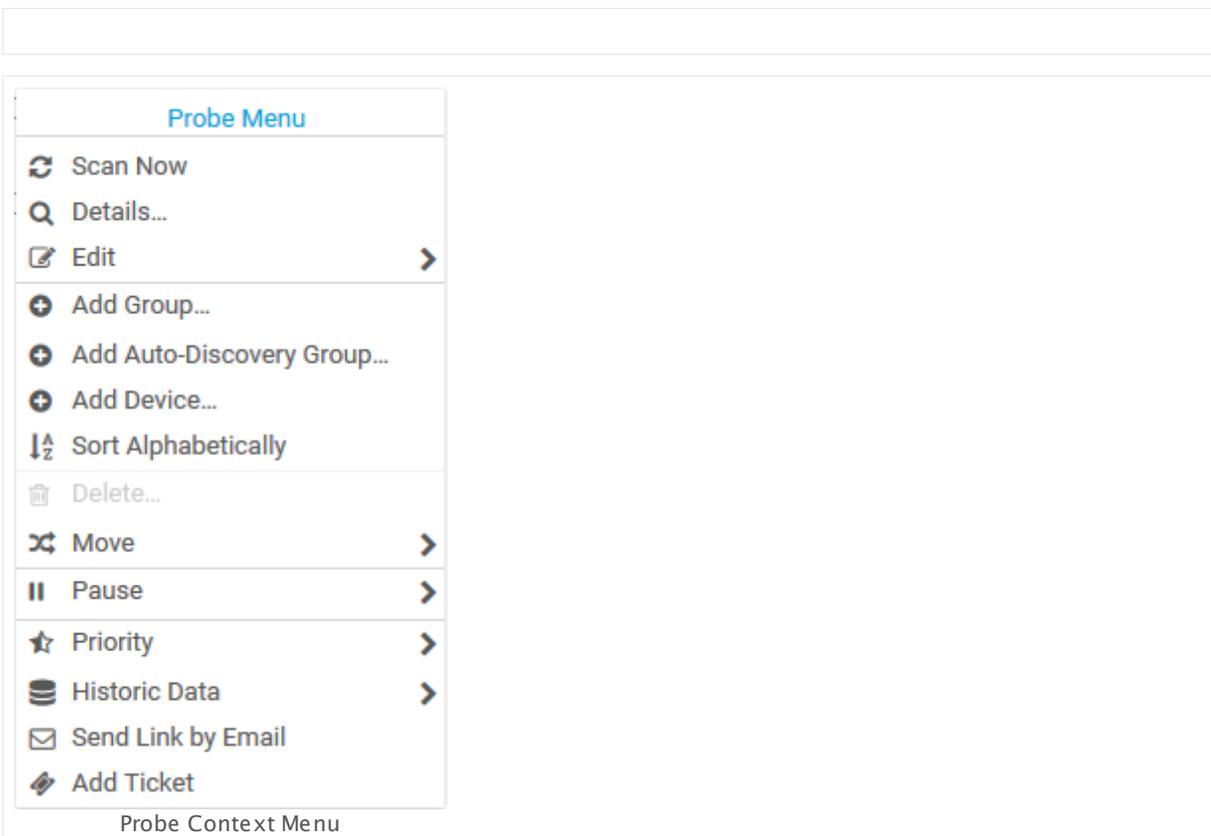
i To view your browser's context menu, hold down the **Ctrl** key (Chrome) or the **Shift** key (Firefox) while right-clicking. You will then see the menu of your browser instead of the PRTG menu. This is not possible with Internet Explorer.

The content of the PRTG context menu varies, depending on the type of object you have selected. See the following subsections for an overview of the available options.

- [Probe Context Menu](#)^[247]
- [Group Context Menu](#)^[251]
- [Device Context Menu](#)^[254]
- [Sensor Context Menu](#)^[259]

Probe Context Menu

The **Probe Menu** contains actions for your [local probe, hosted probe, remote probes, or mini probes](#)^[134].

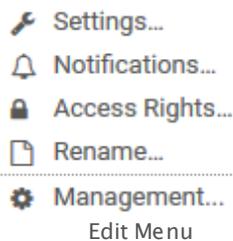


PROBE MENU

Scan Now Perform an immediate scan for the selected probe. This queries the data for all devices and sensors underneath in the [object hierarchy](#) ^[133].

Details... Show the [overview tab](#) ^[198] of the selected probe.

Edit > **Hover** over **Edit** to show the **Edit** menu.



The following actions are available:

- **Settings...**
Open the [Probe Settings](#) ^[351] tab of this probe.
- **Notifications...**
Open the [Notification Triggers](#) ^[326] tab of this probe.
- **Access Rights...**
Open an assistant to edit [User Access Rights](#) ^[158] for this probe.
- **Rename...**
Open an assistant to edit the name of this probe.
- **Management...**
Open the [Management](#) ^[329] tab of this probe.

Add Group... Open an assistant that guides you through the process of adding a new group to the selected probe.

 For detailed instructions, see [Add a Group](#) ^[302].

Add Auto-Discovery Group... Open an assistant that guides you through the process of adding a new auto-discovery group to the selected probe. PRTG creates a new group and runs an auto-discovery in your network to add devices and sensors automatically. For more information, see section [Using the Auto-Discovery](#) ^[282].

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

PROBE MENU

Add Device... Open an assistant that guides you through adding a new device to the selected probe.

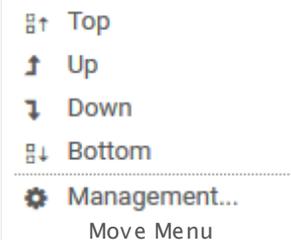
 For detailed instructions, see [Add a Device](#)³¹¹.

Sort Alphabetically Sort direct children (groups and devices) of the selected probe in alphabetical order.

 The ordering is stored in the monitoring configuration and cannot be revoked.

Delete... Delete the selected probe. PRTG will ask for confirmation before anything is actually deleted.

Move > **Hover** over **Move** to open the **Move** menu.



The following actions are available:

- **Top:** Move the probe to the top of the root group.
- **Up:** Move the probe one entry up under the root group.
- **Down:** Move the probe one entry down under the root group.
- **Bottom:** Move the probe to the bottom of the root group.
- **Management...:** Open the [Management](#)³²⁹ tab of the probe.

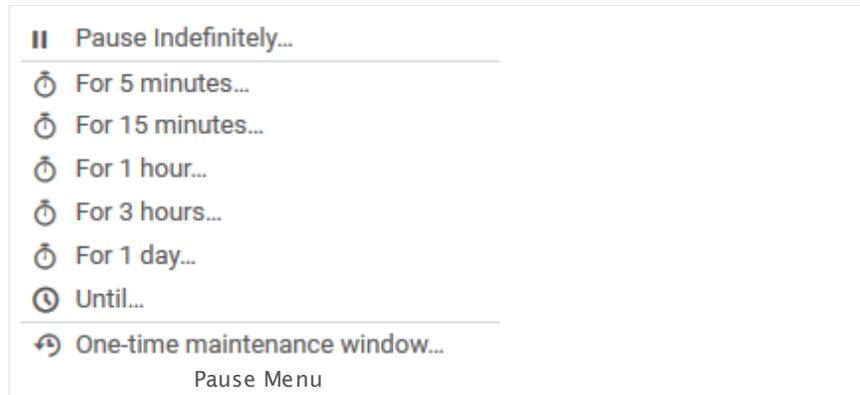
Pause > **Hover** over **Pause** to open the **Pause** menu.

—or—

Resume

If the probe is already in paused or in "simulate error" status, **Resume** appears. **Click** to restart monitoring on this probe.

PROBE MENU



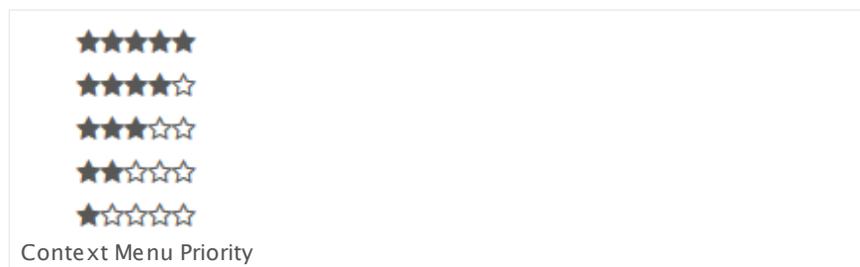
You can pause and resume monitoring on the selected probe. The monitoring for all sensors in the [object hierarchy](#)¹³³ underneath will be paused or resumed.

You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this probe. Use the date time picker to enter the date and time.

Priority >

Hover over **Priority** to open the **Priority** menu.



Define the priority of the selected probe.

 For details, see [Priority and Favorites](#)²⁴².

Historic Data >

Hover over **Historic Data** to open the **Historic Data** menu.

PROBE MENU

-  Last 2 days...
 -  Last 30 days...
 -  Last 365 days...
 -  Create Report...
- Context Menu Historic
Data

The following actions are available:

- Open [the historic data report tabs for the specified interval](#)^[200]: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
 - **Create Report...**: Open an assistant to add a new report to PRTG.
-  For details, see [Reports Step by Step](#)^[3257].

Send Link by Email

Send the link to the selected probe by email. **Click** to create a new email using your system's standard email client. It contains a direct link to the [overview tab](#)^[198] of the selected probe.

Add Ticket

Open the **Add Ticket** dialog.

 For details, see the section [Tickets](#)^[233].

Group Context Menu

The **Group Menu** contains actions for your [groups](#)^[134].

 The context menu of the **Root** group is special and differs from the other groups' menu.

GROUP MENU

Scan Now

Perform an immediate scan for the selected group. This queries the data for all devices and sensors underneath in the [object hierarchy](#)^[133].

Details...

Show the [overview tab](#)^[198] of the selected group.

Edit >

Hover over **Edit** to show the **Edit** menu. The following actions are available:

GROUP MENU

- **Settings...**
Open the [Group Settings](#)^[375] tab of this group.
- **Notifications...**
Open the [Notification Triggers](#)^[3216] tab of this group.
- **Access Rights...**
Open an assistant to edit [User Access Rights](#)^[158] for this group.
- **Rename...**
Open an assistant to edit the name of this group.
- **Management...**
Open the [Management](#)^[329] tab of this group.

Add Group... Open an assistant that guides you through the process of adding a new group to the selected group.

 For detailed instructions, see [Add a Group](#)^[302].

Add Auto-Discovery Group... Open an assistant that guides you through the process of adding a new auto-discovery group to the selected group. PRTG creates a new group and runs an auto-discovery in your network to add devices and sensors automatically. For more information, please see section [Using the Auto-Discovery](#)^[282].

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Add Device... Open an assistant that guides you through adding a new device to the selected group.

 For detailed instructions, see [Add a Device](#)^[311].

Auto-Discovery This option is only available for auto-discovery groups. These are groups with automatic device identification or sensor creation [enabled](#)^[376]. Hover over **Auto-Discovery** to show its menu. The following actions are available:

- **Run Auto-Discovery:** Start an automatic search immediately to automatically add new sensors to the selected device. The search runs in the background and uses the option you set in the **Sensor Management** [section of the group settings](#)^[376]. If found, you see new devices with sensors after a few minutes (if found). For more information, please see [Auto-Discovery](#)^[283] (**Run Auto-Discovery Now**).

GROUP MENU

- **Run Auto-Discovery with Template:** Open an [assistant](#)^[285] to start an automatic search with a desired device template. This is the **Sensor Management** option **Automatic sensor creation using specific device template(s)**. Other automatic device identification options are not available. The option you set in the **Sensor Management** [section of the group settings](#)^[376] will not apply.

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Sort Alphabetically

Sort direct children (groups and devices) of the selected group in alphabetical order.

 The ordering is stored in the monitoring configuration and cannot be revoked.

Delete...

Delete the selected group. PRTG will ask for confirmation before anything is actually deleted.

Clone...

Open an assistant that guides you through cloning the selected group.

 For detailed instructions, see [Clone Object](#)^[3193].

Move >

Hover over **Move** to open the **Move** menu. The following actions are available:

- **Top:** Move the group to the top of the mother node (here usually a probe or another group).
- **Up:** Move the group one entry up under the mother node.
- **Down:** Move the group one entry down under the mother node.
- **Bottom:** Move the group to the bottom of the mother node.
- **To Other Group...:** Move the group to another group to become a sub-group.
- **Management...:** Open the [Management](#)^[329] tab of the group.

Pause >

Hover over **Pause** to open the **Pause** menu.

—or—

If the group is already in paused or in "simulate error" status, **Resume** appears. **Click** to restart monitoring on this group.

Resume

You can pause and resume monitoring on the selected group. The monitoring for all sensors in the [object hierarchy](#)^[133] underneath will be paused or resumed.

GROUP MENU

You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this group. Use the date time picker to enter the date and time.

Priority >

Hover over **Priority** to open the **Priority** menu. Define the priority of the selected group.

 For details, see [Priority and Favorites](#)^[242].

Historic Data >

Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available:

- Open [the historic data report tabs for the specified interval](#)^[200]: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
- **Create Report...**: Open an assistant to add a new report to PRTG.

 For details, see [Reports Step by Step](#)^[3257].

Send Link by Email

Send the link to the selected group by email. **Click** to create a new email using your system's standard email client. It contains a direct link to the [overview tab](#)^[198] of the selected group.

Add Ticket

Open the **Add Ticket** dialog.

 For details, see section [Tickets](#)^[233].

Device Context Menu

The **Device Menu** contains actions for your [devices](#)^[135].

DEVICE MENU

Scan Now

Perform an immediate scan for the selected device. This queries the data for all sensors underneath in the [object hierarchy](#)^[133].

DEVICE MENU

Details...	Show the overview tab ^[198] of the selected device.
Edit >	<p>Hover over Edit to show the Edit menu. The following actions are available:</p> <ul style="list-style-type: none"> ▪ Settings... Open the Device Settings^[402] tab of this device. ▪ Notifications... Open the Notification Triggers^[3216] tab of this device. ▪ Access Rights... Open an assistant to edit User Access Rights^[156] for this device. ▪ Rename... Open an assistant to edit the name of this device. You can also select another device icon.
Add Sensor...	<p>Open an assistant that guides you through adding a new sensor to the selected device.</p> <p> For detailed instructions, see Add a Sensor^[325].</p>
Auto-Discovery	<p>Hover over Auto-Discovery to show the Auto-Discovery menu. The following actions are available:</p> <ul style="list-style-type: none"> ▪ Run Auto-Discovery: Start an automatic search immediately to automatically add new sensors to the selected device. The search runs in the background and uses the option you set in the Sensor Management section of the device settings^[402]. If found, you see new sensors on this device after a few minutes. For more information, please see Auto-Discovery^[283] (Run Auto-Discovery Now). <ul style="list-style-type: none"> ① If you have set the option Manual (no auto-discovery) in the device settings section^[404] Sensor Management and start the auto-discovery from the context menu, PRTG will run it using the standard device identification and change the device setting to Automatic device identification (standard, recommended). Please note that the Enterprise Console^[3473] behaves differently in this case. ▪ Run Auto-Discovery with Template: Open an assistant^[285] to start an automatic search with a desired device template. This is the Sensor Management option Automatic sensor creation using specific device template(s). Other automatic device identification options are not available. The option you set in the Sensor Management section of the device settings^[404] will not apply.

DEVICE MENU

Create Device Template...

Open an assistant that guides you through creating a new device template. The template is then available in [auto-discovery](#) .

 For detailed instructions, see [Create Device Template](#) .

Recommend Now

Start an analysis to get sensor recommendations for this device. When PRTG has finished the inspection of the device, you see the sensor recommendations in a table list on the [device overview tab](#)  where you can add the according sensor types directly.

 This option is only available if the [recommendation engine is enabled](#) .

Sort Alphabetically

Sort the sensors on the selected device in alphabetical order.

 The ordering is stored in the monitoring configuration and cannot be revoked.

Delete...

Delete the selected device. PRTG will ask for confirmation before anything is actually deleted.

Clone...

Open an assistant that guides you through cloning the selected device.

 For detailed instructions, see [Clone Object](#) .

Move >

Hover over **Move** to open the **Move** menu. The following actions are available:

- **Top:** Move the device to the top of the mother node (here usually a probe or group).
- **Up:** Move the device one entry up under the mother node.
- **Down:** Move the device one entry down under the mother node.
- **Bottom:** Move the device to the bottom of the mother node.
- **To Other Group...:** Move the device to another group.

Pause >

Hover over **Pause** to open the **Pause** menu.

—or—

If the device is already in paused or "simulate error" status, **Resume** appears. **Click** to restart monitoring on this device.

Resume

You can pause and resume monitoring on the selected device. The monitoring for all sensors on this device will be paused or resumed.

DEVICE MENU

You can choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this device. Use the date time picker to enter the date and time.

Priority/Favorite ›

Hover over **Priority/Favorite** to open the **Priority/Favorite** menu. Define the priority of the selected device, or add to or remove it from the favorite devices list.

 For details, see [Priority and Favorites](#) ^[242].

Historic Data ›

Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available:

- Open [the historic data report tabs for the specified interval](#) ^[200]: **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
- **Create Report...**: Open an assistant to add a new report to PRTG.

 For details, see [Reports Step by Step](#) ^[3257].

Device Tools ›

Hover over **Device Tools** to open the **Device Tools** menu.

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

-  [Go To Service URL...](#)

-  [New window with HTTP...](#)
-  [New window with HTTPS...](#)
-  [New window with FTP...](#)

-  [Remote Desktop...](#)
- [Traceroute...](#)
- [Install Remote Probe...](#)
- Context Menu Device Tools

The following actions are available:

DEVICE MENU

- **Go To Service URL...**
Open the [service page](#) that you have defined in the [Device Settings](#)^[402]. If there is no service URL available for this device, you can enter an address in the appearing assistant.
 - **New window with HTTP...**
Open a new browser window with Hypertext Transfer Protocol (HTTP) and the IP address / DNS name of the device.
 - **New window with HTTPS...**
Open a new browser window with Hypertext Transfer Protocol Secure (HTTPS) and the IP address / DNS name of the device.
 - **New window with FTP...**
Open a new browser window with File Transfer Protocol (FTP) and the IP address / DNS name of the device.
 - **Remote Desktop...**
Download an [.rdp](#) file. When you execute this file, a remote desktop will start with the IP address / DNS name of the device.
 In Firefox you have to use [mstsc.exe \(Microsoft Terminal Service\)](#) to open the file.
 - **Traceroute...**
Start a traceroute on the selected device. PRTG will display the route and measure transit delays of packets across the IP network.
 - **Install Remote Probe...**
Open an assistant to install a **Remote Probe** of PRTG on this device. For more details, see [Remote Probe Quick Install](#)^[3713].
 This option is only available on devices on local probes.
-  This option is not available in PRTG hosted by Paessler.

Find Duplicates... Search in your PRTG configuration for devices with the same IP address or DNS name as the selected device. A window with the results will appear, either showing existing duplicates or a message indicating that there are no duplicates.

Send Link by Email Send the link to the selected device by email. [Click](#) to create a new email using your system's standard email client. It contains a direct link to the [overview tab](#)^[198] of the selected device.

Add Ticket Open the **New Ticket** dialog.
 For details, see section [Tickets](#)^[233].

Sensor Context Menu

The **Sensor Menu** contains actions for your [sensors](#)^[135].

SENSOR MENU	
Scan Now	Perform an immediate scan for the selected sensor.
Details...	Show the overview tab ^[198] of the selected sensor.
Edit >	<p>Hover over Edit to show the Edit menu. The following actions are available:</p> <ul style="list-style-type: none"> ▪ Settings... Open the Sensor Settings^[428] tab of this sensor. ▪ Notifications... Open the Notification Triggers^[3216] tab of this sensor. ▪ Access Rights... Open an assistant to edit User Access Rights^[158] for this sensor. ▪ Rename... Open an assistant to edit the name of this sensor.
Acknowledge Alarm >	<p>This option is available only in the sensor menu when you select a sensor in a Down or Down (Partial) status^[195].</p> <p>You can acknowledge an alarm for the selected sensor. An acknowledged alarm will show up in the alarms list as "acknowledged" (see Sensor States^[195]) and will not trigger^[3170] any more notifications^[3216].</p> <p>You can choose between: Acknowledge Indefinitely..., acknowledge For 5 Minutes..., For 15 Minutes..., For 1 Hour..., For 3 Hours..., For 1 Day..., or Until... If you choose Until... an assistant appears where you can define a date. Use the date time picker to enter the date and time. If the alarm condition still exists after this date, the sensor will show a Down status again.</p> <p>i If the alarm condition clears, the sensor usually returns into an Up status immediately with the next sensor scan. For details about acknowledging an alarm, see Alarms^[220] section.</p>
Delete...	Delete the selected sensor. PRTG will ask for confirmation before anything is actually deleted.
Clone...	Open an assistant that guides you through cloning the selected sensor.

SENSOR MENU

 For detailed instructions, see [Clone Object](#) ^[3193].

Move ›

Hover over **Move** to open the **Move** menu. The following actions are available:

- **Top:** Move the sensor to the top of the device on which it runs.
- **Up:** Move the sensor one entry up on the device.
- **Down:** Move the sensor one entry down on the device.
- **Bottom:** Move the sensor to the bottom of the device.

Pause ›

Hover over **Pause** to open the **Pause** menu.

—or—

Resume

If the sensor is already in [paused status](#) ^[195] or in **Simulate Error Status**, **Resume** appears. **Click Resume** to restart monitoring on this sensor.

You can pause and resume monitoring of the selected sensor. Choose between: **Pause Indefinitely...**, pause **For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Pause Until...**. If you choose **Pause Until...**, an assistant appears where you can define a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can directly add a **One-time maintenance window** to pause monitoring during a planned downtime. In the appearing assistant, define the start and end date of the maintenance window for this sensor. Use the date time picker to enter the date and time. Inheritance of the **Schedules, Dependencies, and Maintenance Window** setting from a parent device, group, or probe will be suspended for this timeframe and set again afterwards.

Simulate Error Status

Set the selected sensor to a [Down status](#) ^[195]. Like for the paused status, **Resume** will appear in the context menu if a the selected sensor is already in a simulated error status.

 "Simulate error status" does not work for sensors that run on a PRTG Mini Probe.

Priority/Favorite ›

Hover over **Priority/Favorite** to open the **Priority/Favorite** menu. Define the priority of the selected sensor, or add or remove it from the favorite devices list.

 For details, see [Priority and Favorites](#) ^[242].

Historic Data ›

Hover over **Historic Data** to open the **Historic Data** menu. The following actions are available:

SENSOR MENU

- Open the [historic data tab for the specified interval](#)²⁰¹: **Live Data...**, **Last 2 days...**, **Last 30 days...**, or **Last 365 days...**
- **View Historic Data**: Open the [Historic Data](#)²⁰⁴ tab of this sensor.
- **Create Report...**: Open an assistant to add a new report to PRTG.

 For details, see [Reports Step by Step](#)³²⁵⁷.

Send Link by Email

Send the link to the selected sensor by email. **Click** to create a new email using your system's standard email client. It contains a direct link to the [overview tab](#)¹⁹⁸ of the selected sensor.

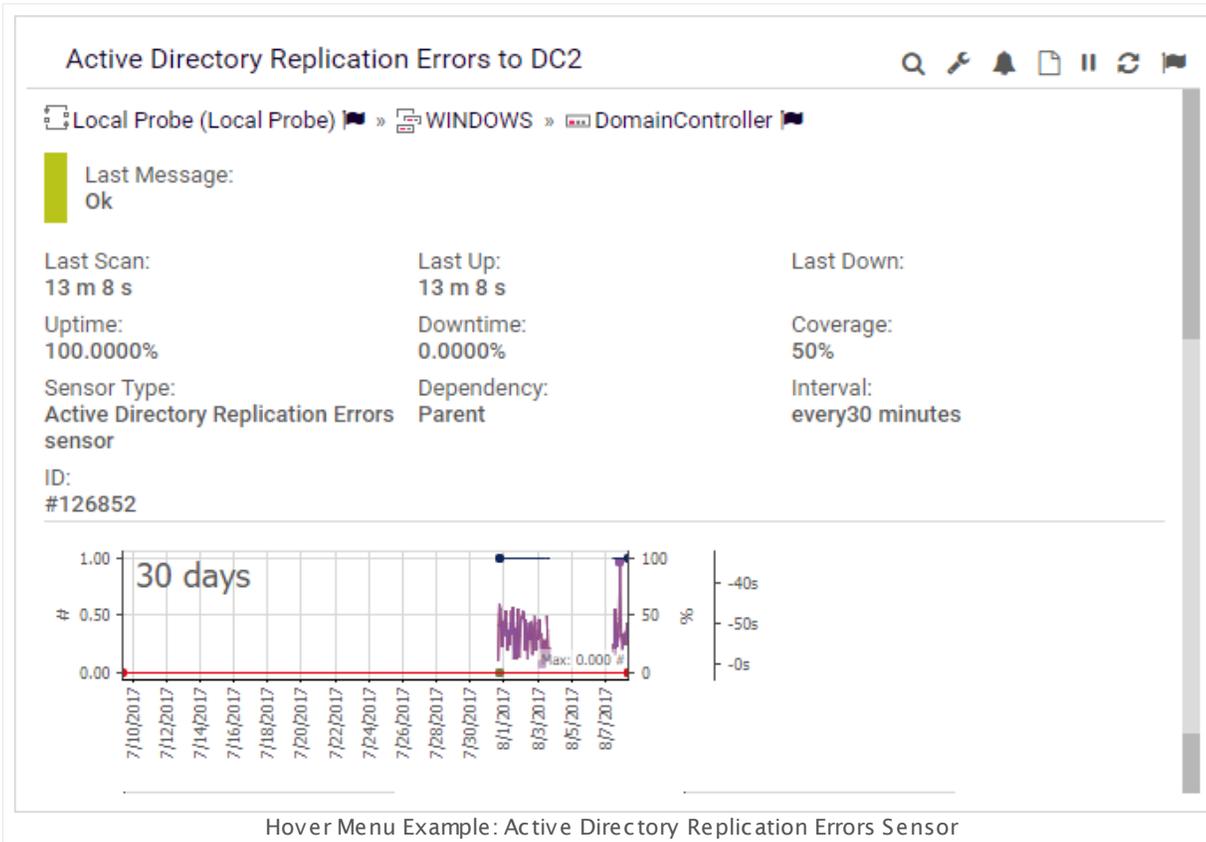
Add Ticket

Open the **Add Ticket** dialog.

 For details, see section [Tickets](#)²³³.

6.20 Hover Popup

Whenever you rest the mouse pointer for a second over an object's icon in the [device tree](#)^[181], a hover popup window will appear, showing details about this object. It contains information from the object's [overview tab](#)^[198], as well as several graphs. The exact information provided depends on the kind of object you are hovering over.



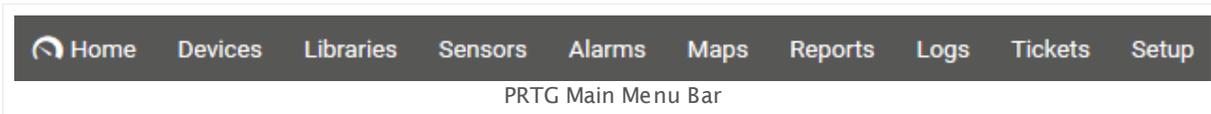
- ❗ The hover popup only appears if your browser is the currently focused window on your desktop. It disappears with every (automatic) page refresh.

Menu Icons

At the top of the hover popup window, several icons are shown that enable you to view or edit the current object. These are the most important options from this object's [context menu](#)^[247], which is shown when right-clicking it.

6.21 Main Menu Structure

You can access all functions of PRTG using the main menu. In this section, you find descriptions about the most important menu items. Often, you can either **click** an item directly, or **hover** over it to show more items.



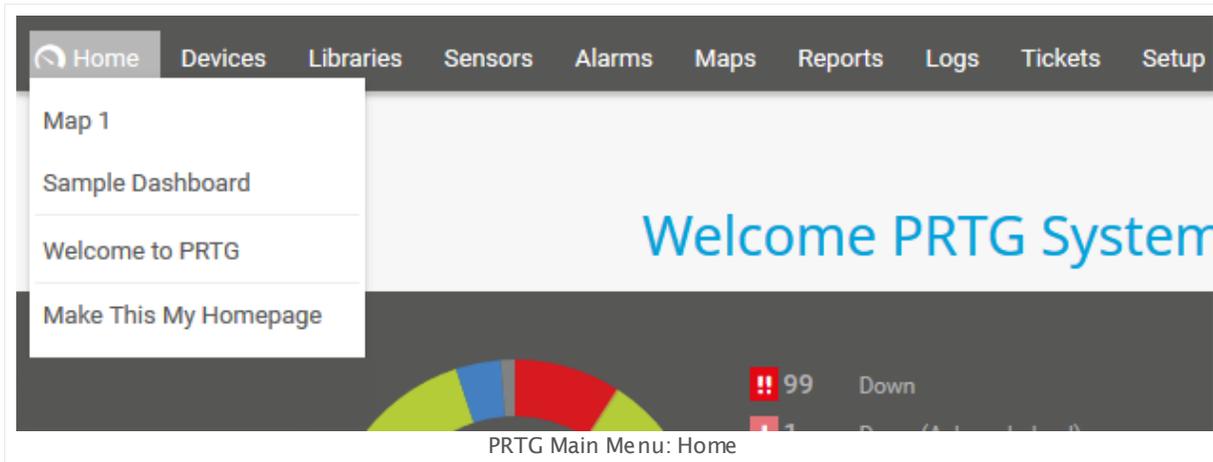
i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

The following menu items are available:

- [Home](#) ²⁶³
- [Devices](#) ²⁶⁵
- [Libraries](#) ²⁶⁷
- [Sensors](#) ²⁶⁷
- [Alarms](#) ²⁷⁰
- [Maps](#) ²⁷¹
- [Reports](#) ²⁷²
- [Logs](#) ²⁷³
- [Tickets](#) ²⁷⁴
- [Setup](#) ²⁷⁵
- [Search Box](#) ²⁷⁷
- [Logout \(Off Symbol\)](#) ²⁷⁸

Home

Click to open the user's homepage. The default setting is the [PRTG welcome page](#) ¹⁸¹. You can change the homepage in the user [account settings](#) ³³⁰⁴. Point to **Home** to show other menu items.



HOME

Sample Dashboard

Open a preconfigured dashboard to view monitoring data in another layout. Dashboards provide different preset overviews with the status of your sensors. This dashboard is one of the default [Maps](#) that PRTG creates automatically with a new installation.

i The **Home** menu shows maps that have a 5***** [priority](#). To show a desired map here, give it 5 stars on the [maps overview page](#). You can include up to 10 map entries in the menu. For details, see section [Maps in Home Menu](#).

i You can change the appearance of the default dashboard with the [Map Designer](#). To not show the sample dashboard in the menu, define a [priority](#) lower than 5***** for this map.

☁ This option is not available in PRTG hosted by Paessler.

Switch Cluster Node >

This option is only available if PRTG runs in [Clustering](#) mode. Show available cluster nodes. **Hover** over **Switch Cluster Node** to show other menu items. Follow the menu path (it is specific to your setup) to select another cluster node. The current Master node is shown in bold letters. Click on a node's name to leave the current node and connect to the other, showing the same page there.

☁ This option is not available in PRTG hosted by Paessler.

Welcome to PRTG

Open the [Welcome Page](#) that shows the Paessler news feed and various information about your PRTG installation, and it provides quick links to major sections of the web interface.

i This is the default homepage of the PRTG web interface.

HOME

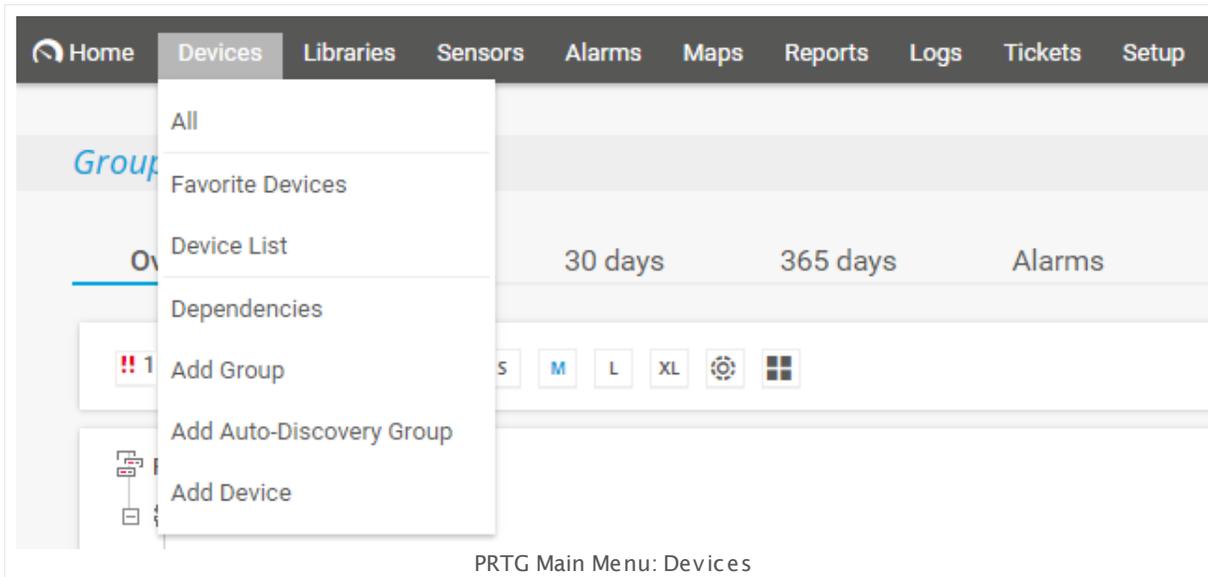
Make This My Homepage

Change the page that is loaded when you click **Home** in the main menu. Select this command on any page to set its URL as the current user's homepage. This setting is user sensitive. The default homepage is [/welcome.htm](#).

You can change this setting any time by clicking this command again, or by changing the **Homepage URL** in the [My Account](#) ^{330d} settings.

Devices

Click to show a group view of all your devices, starting with the **Root** group, which contains all other groups of your setup. **Hover** over **Devices** to show other menu items.



DEVICES

All

Open the **Overview** tab of the [Root](#) ^{133d} group that shows a group view of all your devices (the device tree).

Favorite Devices

Open a table list of all devices marked as [Favorite](#) ^{242d}. **Click** the **Print QR-Codes** button to show a printable list of the QR codes of all your favorite devices.

i To mark any device as a favorite device, select **Priority/ Favorite | Add to Favorites** from its context menu or click the small flag on a device's details page.

DEVICES

Device List

Open a list view of all devices in your setup. **Click** to show a table list of all devices in your setup.

 In the [table list](#)^[237] that appears, you can re-sort the items by clicking the column's header items.

Dependencies

Open an overview list of the [Dependencies](#)^[141] configured for the objects in your setup. You can select dependencies and define master dependencies in the **Schedules, Dependencies, and Maintenance Windows** [settings of a monitoring object](#)^[217] (not available for the **Root** group).

Add Group

Start an assistant that guides you through the process of adding a new group to your setup.

 For more information, see section [Create Objects Manually](#)^[301].

 You can create new groups much faster by choosing **Add Group...** from a probe's or group's context menu.

Add Auto-Discovery Group

Start an assistant that guides you through the process of adding a new auto-discovery group to your setup. PRTG will create a new group and run an auto-discovery in your network to add devices and sensors for these devices automatically.

 For more information, see section [Using the Auto-Discovery](#)^[282].

 You can create new groups much faster by choosing **Add Auto-Discovery Group...** from a probe's or group's context menu.

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Add Device

Start an assistant that guides you through the process of adding a new device to an existing group. During the process, you can choose if PRTG will run an auto-discover for the new device to add sensors automatically.

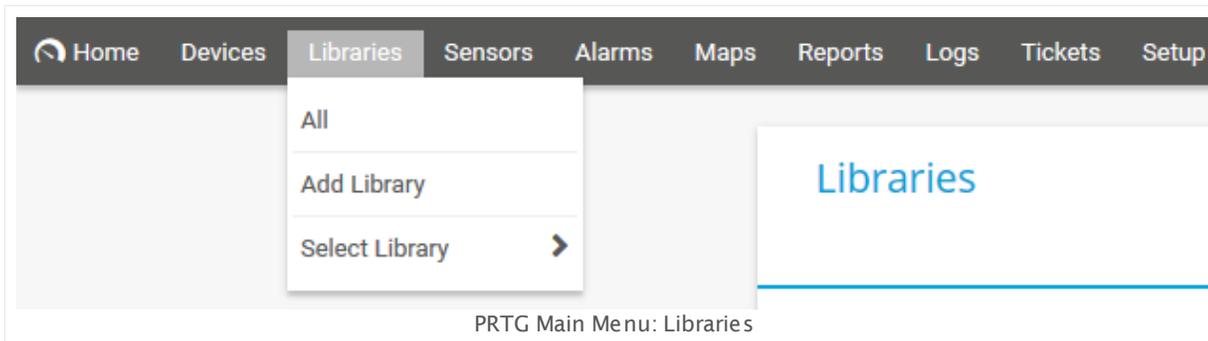
 For more information, see section [Create Objects Manually](#)^[301].

 You can create new devices much faster by choosing **Add Device...** from a group's context menu.

Libraries

Click to open the **Libraries** overview list where you can view or add custom views of your network status and monitoring data. Hover over **Libraries** to show other menu items.

For more information, see [Libraries](#) section.



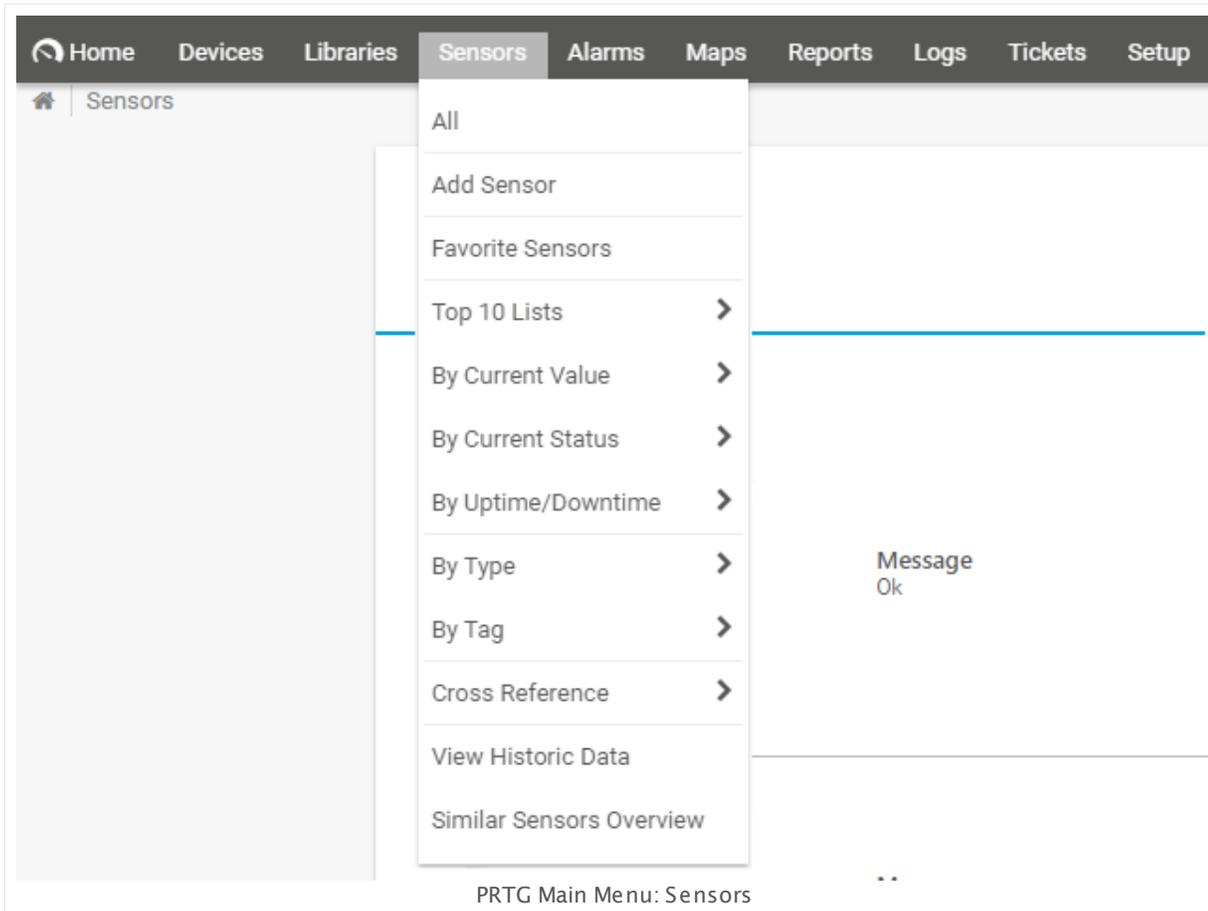
LIBRARIES

All	Open the Libraries overview list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open an assistant to create a new library.
Select Library >	Open an existing library. Hover over Select Library to show more options. Follow the alphabetical menu path (it is specific to your setup) to view your libraries. Click a library to open it.

Sensors

Click to show a table list of all [sensors](#). In the [table list](#) that appears, you can re-sort the items by clicking the column's header items and you can filter the list by related object and tag with the inline filter directly above the table. Hover over **Sensors** in the main menu bar to show other menu items.

- The column **Last Value** shows only the last value of the sensor's **primary channel**.
- For most sensor lists, you can use [Multi-Edit](#) to change the settings of more than one sensor at once.



SENSORS

All

Open a [table list](#)^[237] of all [sensors](#)^[135]. In the table list appearing, you can re-sort the items by clicking the column's header items.

- ⓘ The column **Last Value** shows only the last value of the sensor's **primary channel**.

Add Sensor

Start an assistant that guides you through the process of adding a new sensor to an existing device. For more information, see section [Add a Sensor](#)^[325]. During the process, you can also choose to create a new device via the [Add a Device](#)^[317] assistant (that you can also open from the ["Devices" menu](#)^[265] directly).

Favorite Sensors

Open a table list of all sensors that you marked as [Favorite](#)^[242].

- ⓘ To mark any sensor as a favorite sensor, select **Priority/ Favorite | Add to Favorites** from its context menu or click the small flag on a device's details page.

SENSORS

Top 10 Lists >

Open a dashboard view with different top 10 lists that show best or worst uptime, Ping, bandwidth usage, website response times, CPU usage, disk usage, memory usage, and system uptime. **Click** to show top 10 lists for all sensors. **Hover** over **Top 10 Lists** to show other menu items. Follow the menu path (it is specific to your setup) to view top 10 lists for a specific probe or group only.

 The shown sensors are selected by default tags.

By Current Value >

Open a list of sensors filtered by value. **Hover** over **By Current Value** to show other menu items. Follow the menu path to view [table lists](#)^[237] of **Fastest Value** or **Slowest Value** sensors for

- Ping
- Port
- Webpages
- IMAP/POP3/SMTP
- FTP

as well as a list of sensors with **Highest Value** or **Lowest Value** regarding

- Bandwidth
- CPU
- Disk
- Memory

 The shown sensors are selected by default tags.

By Current Status >

Open a list of sensors filtered by status. **Hover** over **By Current Status** to show other menu items. Follow the menu path to view [table lists](#)^[237] of all sensors in a certain status.

 For more information about sensor states, see [Sensor States](#)^[195] section.

By Uptime/Downtime >

Open a list of sensors filtered by different parameters. **Hover** over **By Uptime/Downtime** to show other menu items. Follow the menu path to view [table lists](#)^[237] of all sensors sorted by

- Best Uptime (%)
- Highest Uptime (Time)
- Worst Downtime (%)
- Highest Downtime (Time)

SENSORS

By Type ›

Open a list of sensors filtered by [sensor type](#)^[429]. **Hover** over **By Type** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to view a sensor [table list](#)^[237] containing only sensors of one specific sensor type.

By Tag ›

Open a list of sensors filtered by [tag](#)^[139]. **Hover** over **By Tag** to show other menu items. Follow the alphabetical menu path (it is specific to your setup) to see available tags. Select a tag to view a [table list](#)^[237] containing only sensors marked with this tag.

 If you have more than 1000 tags, no tags are shown here. See [Tags](#)^[140] section for more information.

Cross Reference ›

Open the sensor cross reference to show information about all sensors including [priority and favorite status](#)^[242], [scanning interval](#)^[345], [access rights](#)^[158], [notification trigger settings](#)^[217], [schedule](#)^[142], and [dependency](#)^[141]. **Click** to show a sensor cross reference for all sensors. **Hover** over **Cross Reference** to show other menu items. Follow the menu path (it is specific to your setup) to view cross reference information for sensors by type or tag.

View Historic Data

Open an assistant for a quick generation of sensor data reports.

 For more information, see [Historic Data Reports](#)^[204] section.

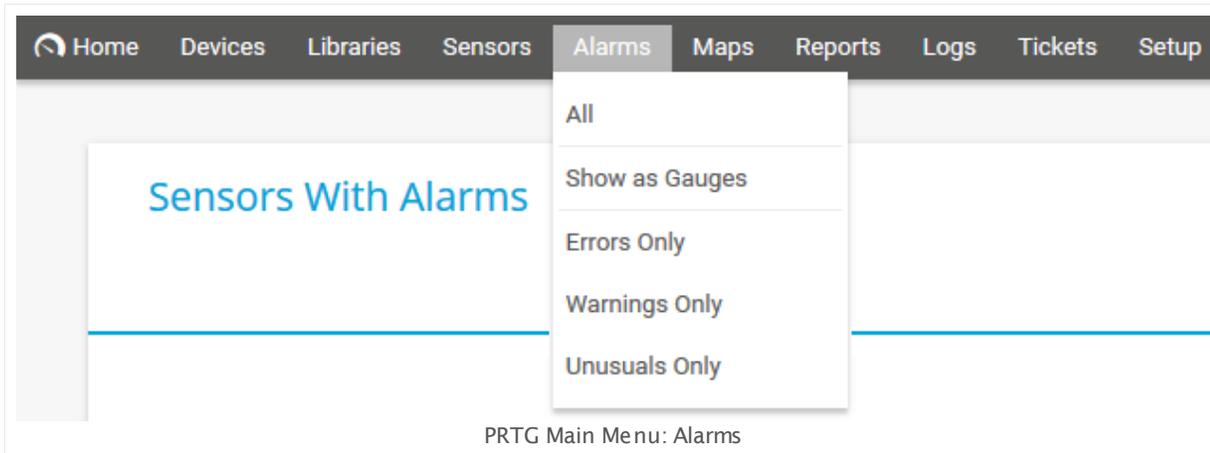
Similar Sensors Overview

Open an overview page with a list of similar sensors.

 For more information, see [Similar Sensors](#)^[209] section.

Alarms

Click to show all sensors that currently show a **Down**, **Down (Partial)**, **Warning**, or **Unusual** status. In the [table list](#)^[237] that appears, you can re-sort the items by clicking the column's header items. If you select **Show as Gauges**, this command displays the [sensor gauges](#)^[198] in a size corresponding to their priority. **Hover** over **Alarms** to show other menu items.



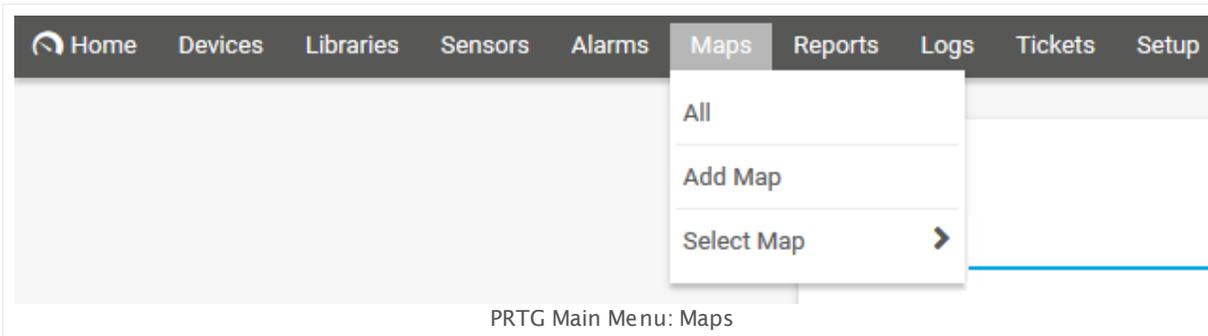
ALARMS

All	Open a list of all sensors that are currently in Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status ¹⁹⁵ .
Show as Gauges	Open a page with the gauges of all sensors that are currently in Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. The size of the sensor gauges corresponds to their respective priority.
Errors Only	Open a list of all sensors that are currently in Down, Down (Partial), or Down (Acknowledged) status.
Warnings Only	Open a list of all sensors that are currently in Warning status.
Unusuals Only	Open a list of all sensors that are currently in Unusual status.

Maps

Click to open the **Maps** overview page where you can view or add custom views of your network status and monitoring data. **Hover** over **Maps** to show other menu items.

 For more information, see [Maps](#) ³²⁷⁶ section.



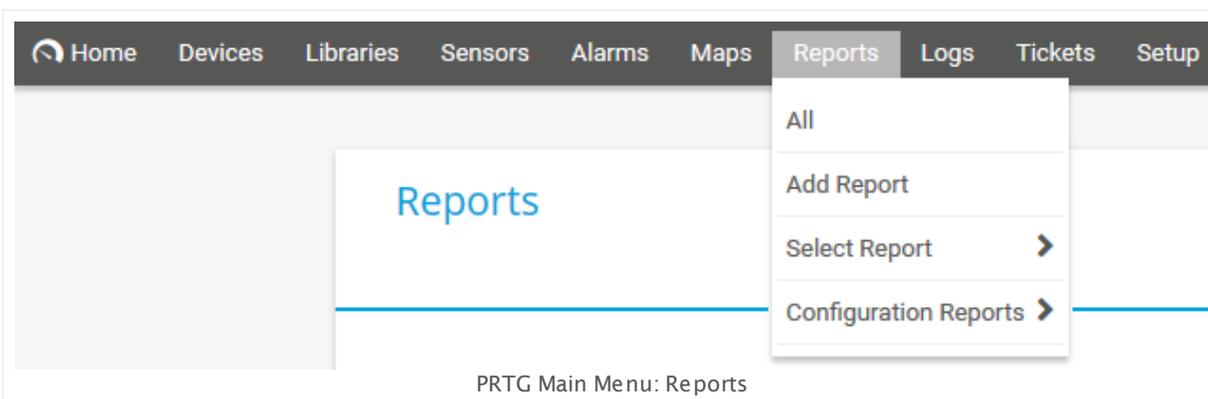
MAPS

- All** Open the **Maps** overview page where you can view or add custom views of your network's status and monitoring data.
- Add Map** Open an assistant to directly [add](#) a new map.
- Select Map >** Open an existing map. **Hover** over **Select Map** to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Reports

Click to open the **Reports** overview page where you can view or add reports of your monitoring data. **Hover** over **Reports** to show other menu items.

 For more information, see [Reports](#) section.



REPORTS

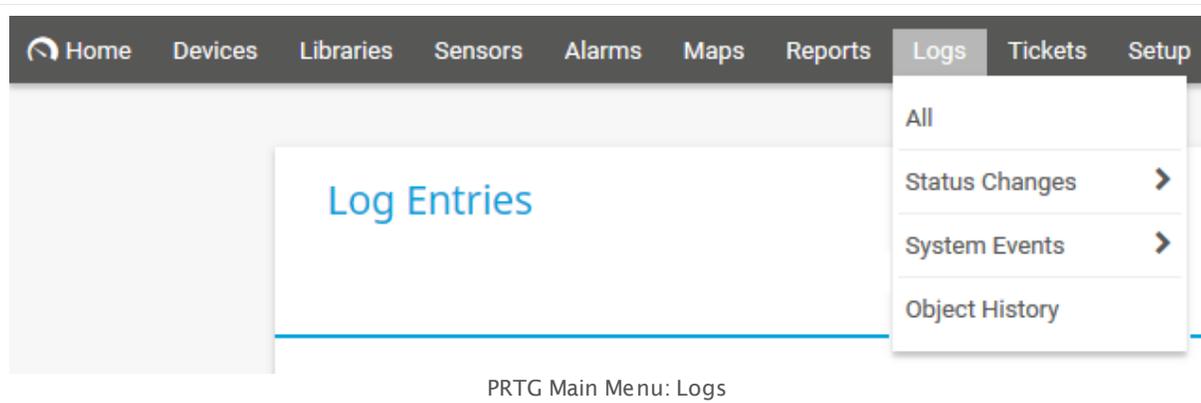
All	Open the Reports overview page where you can view or add reports of your monitoring data.
Add Report	Open an assistant to directly add a new report.
Select Report ›	Open an existing report. Point to Select Report to show other menu items. Follow the menu path (it is specific to your setup) to select a report.
Configuration Reports ›	Create reports for maps, reports, users & user groups, and system configuration to document changes to the configuration. Point to Reports Configuration Reports to see the available configuration reports .

Logs

Click to show log information for all objects in your configuration, newest first. In the [table list](#) appearing, you can filter the items by using the [respective options](#). **Hover** over **Logs** to show other menu items.

For more information, see [Logs](#) section.

Logs for monitoring objects (for example, sensors) are available as long as you define **Logfile Records** in the **Historic Data Purging** settings under [System Administration—Core & Probes](#).



LOGS

All	Open a table list with log information for all objects in your configuration, newest first.
-----	---

LOGS

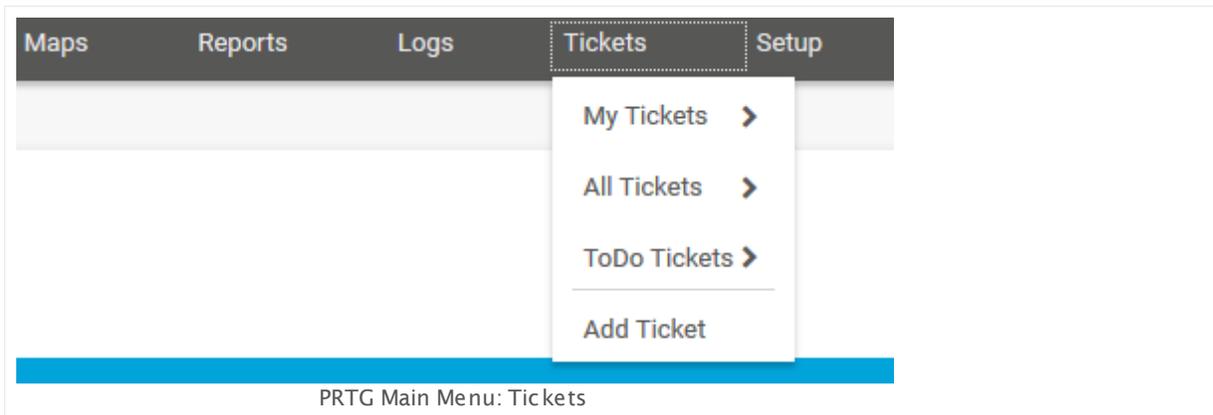
- Status Changes** › Open a list with log information for certain status changes only. **Hover** over **Status Changes** to show other menu items. Follow the menu path to view log entries with a special value in the **Status** field only. Select between **Up & Down** (shows entries with either **Up** or **Down** in the **Status** field), **Down, Warning, Unusual, Up, Paused/Resumed** (shows entries with either **Paused** or **Resumed** in the **Status** field), or **Acknowledged Alarms**.
- System Events** › Open a list with log information regarding certain system event types only. **Hover** over **System Events** to show other menu items. Select between the following event types: **Probe Related, Cluster Related, Auto-Discovery, Notifications, or Status Messages**.
- Object History** Open a list with log information about changes to the PRTG setup and deletions of subordinate system objects. The object history page has a tab-like interface. Using the tabs you can navigate through various sub-pages in order to view the changes to all related settings and deletions of objects. Select between the following tabs: **My Account, System Administration, Notifications, Schedules, User Accounts, User Groups, Reports, Libraries, or Maps**.
-  You can open a specific tab directly with the context button **History** in the [page header bar](#)¹⁸⁵ on the corresponding pages.

Tickets

Click to show all open tickets that are assigned to the current user. In the [table list](#)²³⁷ that appears, you can re-sort the items by clicking the column's header items, and you can filter the list with the inline filter directly above the table. **Hover** over **Tickets** to show other menu items.

Tickets show important system information or action steps to take for the administrator. For best experience with PRTG, check every ticket and conduct appropriate actions.

 For more information, see section [Tickets](#)²³⁰.



You have several options to display a list of tickets, which is filtered to your needs. You can also create a new ticket via the main menu.

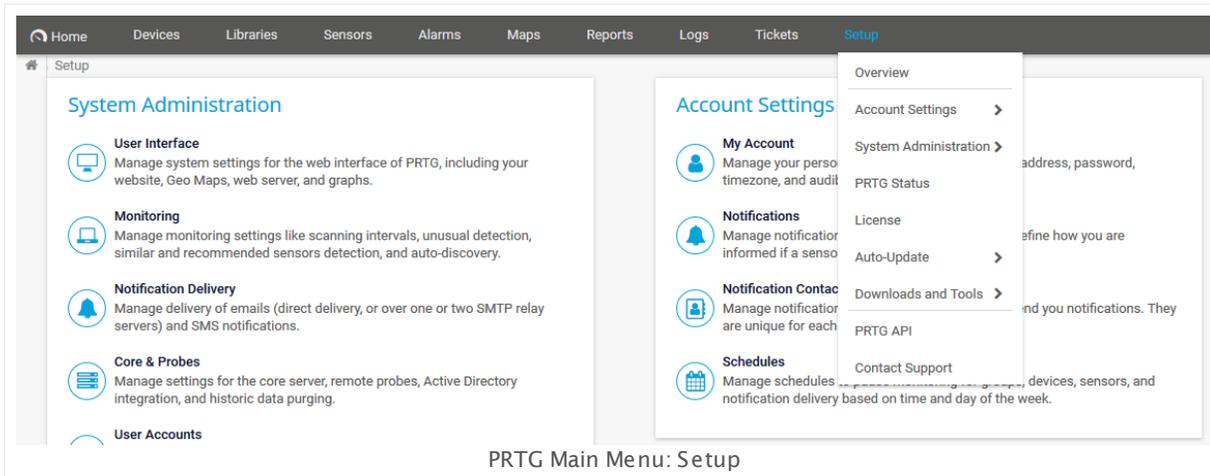
TICKETS	
My Tickets ›	Open a list of all open tickets that are assigned to the current user. Hover over My Tickets to show other menu items for filtering these tickets depending on their status.
All Tickets ›	Open a list of all open tickets of all PRTG users. Hover over All Tickets to show other menu items for filtering these tickets depending on their status.
ToDo Tickets ›	Open a list of open tickets from the type ToDo . Hover over ToDo Tickets to show other menu items for filtering these tickets depending on their status.
Add Ticket	Open the Add Ticket dialog. Provide the needed information and confirm by clicking OK to create a User Ticket .
	 For more information about available options, refer to section Tickets ²³⁰ .

Setup

Click to show the setup page. **Hover** over **Setup** to show other menu items.

 For more information, see [Setup](#) ³³⁰² section.

Part 6: Ajax Web Interface—Basic Procedures | 21 Main Menu Structure



PRTG Main Menu: Setup

SETUP

Overview

Open the [setup page](#) ³³⁰².

Account Settings >

Open the [My Account](#) ³³⁰⁴ settings. **Hover** over **Account Settings** to show and open the tabs of account settings directly. Choose from:

- [My Account](#) ³³⁰⁴
- [Notification Templates](#) ³³¹¹
- [Notification Contacts](#) ³³³⁴
- [Schedules](#) ³³³⁸

System Administration >

Open the [System Administration](#) ³³⁴³ settings. **Hover** over **System Administration** to show and open the tabs of the system administration settings directly. Choose from:

- [Manage Subscriptions](#) ⁷¹ (PRTG hosted by Paessler only)
- [User Interface](#) ³³⁴³
- [Monitoring](#) ³³⁵⁵
- [Notification Delivery](#) ³³⁶¹
- [Core & Probes](#) ³³⁶⁶
- [Cluster](#) ³³⁹⁴ (PRTG on premises only)
- [User Accounts](#) ³³⁷⁶
- [User Groups](#) ³³⁸³
- [Administrative Tools](#) ³³⁸⁸

SETUP

PRTG Status

Open the [PRTG Status—System Status](#)³³⁹⁶ page. When running a cluster, **hover** over **PRTG Status** to show other menu items. Choose from:

- [System Status](#)³³⁹⁶
- [Cluster Status](#)³⁴¹²

License

Open the [license activation status](#)³⁴¹⁴ page.

 This option is not available in PRTG hosted by Paessler.

Auto-Update ›

Open information about the [Software Auto-Update](#)³⁴⁰⁷ status of your PRTG installation. On this page, you can also download and install available updates. **Hover** over **Auto-Update** to show other menu items. Choose from:

- [Status](#)³⁴⁰⁷ to view the update status and to manually check for the latest update.
- [Settings](#)³⁴⁰⁹ to define your update settings.

 This option is not available in PRTG hosted by Paessler.

Downloads and Tools›

Open the [downloads page](#)³⁴²⁰ of PRTG for additional downloads and tools. Choose from:

- [Client App for Windows \(Enterprise Console\)](#)³⁴²⁰  (PRTG on premises only)
- [Client Apps for Mobile Devices](#)³⁴²⁰
- [Remote Probe Installer](#)³⁴²⁰
- [PRTG Tools](#)³⁴²⁰

PRTG API

Open the [Application Programming Interface \(API\) Definition](#)³⁶⁰⁶ for your installation.

Contact Support

Open the [Contact Paessler Support / Send Your Feedback to Paessler](#)³⁴²⁴ form.

Search (Reading-glass Symbol)

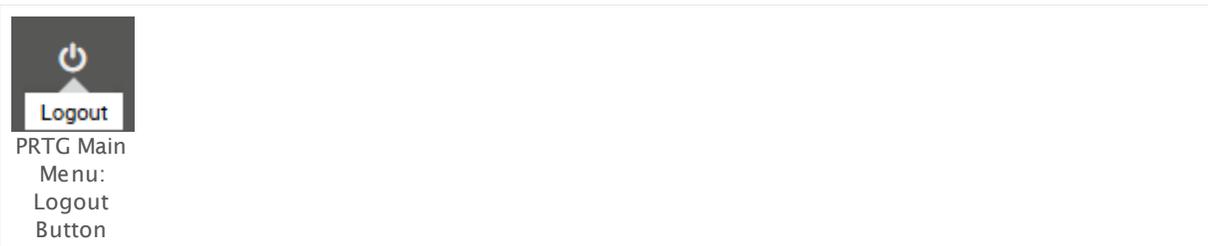
Search... 

PRTG Main Menu: Search Box

Click the **Search** box to find objects in your monitoring setup. Enter your search term, and start the search with the enter key. PRTG will perform a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments, as well as in the PRTG user manual. You will see all search results on a new page.

i You can only search for names that are actually displayed. For example, to search for a specific user, use their display name. The login name or email address of a user account will not be used.

Logout (Off Symbol)



Log out the current user and return to the [login screen](#)¹⁶⁸.

Context Menu

Additionally, there are [Context Menus](#)²⁴⁷ available for all objects. Right-click an object to open it.

Part 7

Ajax Web Interface—Device and Sensor Setup

7 Ajax Web Interface—Device and Sensor Setup

The PRTG web interface is the feature complete access to PRTG Network Monitor via the web. Use the PRTG web interface as default interface to setup your monitoring and bring it to perfection.

Configure devices and sensors, set up notifications, review monitoring results, create reports, visualize your monitoring on dashboards, and use many more PRTG features to complete your monitoring.

The PRTG web interface is based on Asynchronous Java Script and XML (AJAX) and designed to optimally adjust to your systems by its **responsive design**. It shows all object setting dialogs as pop-up layers, so you never lose the current context. The web interface adjusts to the size of your screen, so you always get information displayed in an optimized way.

While you are [logged in](#)¹⁶⁸, the PRTG web interface continuously refreshes the data on the screen via AJAX calls and you always are up to date on the current monitoring results. You can [set](#)³³⁷⁶ the refresh interval and method individually.

Thanks to **Single Page Application (SPA)** technology, your system will stay highly performant because only single page elements are refreshed when necessary.

The following sections introduce device and sensor setup in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Device and Sensor Setup—Topics

- [Auto-Discovery](#)²⁸²
- [Create Objects Manually](#)³⁰¹
- [Manage Device Tree](#)³²⁹
- [Root Group Settings](#)³³¹
- [Probe Settings](#)³⁵¹
- [Group Settings](#)³⁷⁵
- [Device Settings](#)⁴⁰²
- [Sensor Settings](#)⁴²⁸—[List of Available Sensor Types](#)⁴²⁹
- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵
- [Sensor Channels Settings](#)³¹⁶⁰
- [Sensor Notification Triggers Settings](#)³¹⁷⁰

Other Ajax Web Interface Sections

- [Ajax Web Interface—Basic Procedures](#)¹⁶⁶
- [Ajax Web Interface—Advanced Procedures](#)³¹⁸⁴

Related Topics

- [Enterprise Console](#) 
- [PRTG Apps for Mobile Network Monitoring](#) 

7.1 Auto-Discovery

The PRTG auto-discovery is a great way to automatically create a sophisticated and concise set of sensors for your complete network. It is mainly suitable for LAN discovery because it involves a lot of SNMP and WMI.

-  PRTG already runs a quick initial auto-discovery as soon as you finish the installation of PRTG to automatically show you several available devices in your network.

How Auto-Discovery Works

The PRTG auto-discovery process has three stages:

- **Step 1**
Scanning a network segment for devices using Ping (for groups only).
- **Step 2**
Assessing the device type for all devices discovered in step 1 (using SNMP, WMI, and other protocols).
- **Step 3a**
Creating sensor sets that match the discovered device types of step 2. This is done based on built-in device templates with recommended sensors for many device types.

Step 3b (optional)

Creating sensor sets using device templates that PRTG users created (see [Create Device Template](#)³²⁰³ section).

You can use the auto-discovery on group level for a range of IP addresses, or for individual devices that you have created manually. You can run the auto-discovery just once, on demand via the context menu, or scheduled every hour, day, or week. Running the auto-discovery daily or weekly on group level automatically creates new devices when they are connected to the network and adds according sensors.

-  PRTG will create a notifying [ticket](#)²³⁰¹ when at least one new device or sensor has been discovered. You will also receive a ticket in case of an error. By default, PRTG sends tickets as email as well. You can change this behavior in your user account settings, section [Ticket System](#)³³⁰⁹.

Restrictions

Please be aware of the following restrictions of the auto-discovery:

- PRTG cannot discover devices that cannot be pinged, because step 1 uses pings. If, for example, a firewall blocks echo requests, PRTG cannot discover a device behind it.
- Please define authentication settings for **Windows Systems, Linux (SSH/WBEM) Systems, VMware/XEN Servers, SNMP Devices, Database Management Systems, and Amazon CloudWatch** to fully benefit from the power of this feature. We recommend that you define these settings in the [Root group](#)³³¹¹.
- If a device has more than one IP address, it may show up more than once in the discovery results, even though PRTG tries to identify these situations.

- Auto-discovery on group level will not create new sensors on devices that already exist in PRTG but only on newly discovered devices. If you want to automatically add sensors to an existing device, please run the auto-discovery on this device.
 - Using frequent auto-discoveries of large network segments can lead to performance issues. Because of this we recommend that you only schedule regular auto-discoveries where necessary. For detailed information, see this Knowledge Base article: [Why can automatic auto-discoveries evoke performance issues?](#)
 - PRTG automatically adds suitable device icons to discovered devices. PRTG uses a device's MAC address for this purpose, which it determines via **ARP (Address Resolution Protocol)**. This only works via IPv4 and not with IPv6. Usually, ARP works only in the local network unless your router supports ARP and you configure it accordingly.
 - If you use [Multi-Edit](#)³¹⁹⁷ to automatically create sensors using specific device template(s), the auto-discovery is not automatically started. To manually start the auto-discovery, right-click the individual devices and select **Auto-Discovery | Run Auto-Discovery**.
- i** HTTP sensors indicate the access type to the target device with their names (**HTTP**, **HTTP (8080)**, and **HTTPS**). This approach helps to distinguish HTTP sensors if the auto-discovery adds more than one instance to a device.

Run Auto-Discovery Now

You can run an auto-discovery at any time for a group or a device. To do so, **right-click** the object to analyze and select **Run Auto-Discovery** from the [context menu](#)²⁴⁷. PRTG immediately starts searching for new objects that can be added to the device tree. If you use it for an auto-discovery group (not available on hosted probes), PRTG will add devices with according sensors, if found. If you use it for a device, PRTG will add new sensors, if found. You can always see in the corresponding [page header bar](#)¹⁸⁵ when PRTG ran the last auto-discovery on a selected group or device.

- i** The auto-discovery will also re-add devices or sensors you have manually deleted. If you do not want this, please create objects [manually](#)³⁰¹ only.

Creating an Auto-Discovery Group

There are several ways to start auto-discovery:

- Select **Devices | Add Auto-Discovery Group** from the [main menu bar](#)²⁶³. To start an automatic detection of devices and sensors in your network an assistant will appear, leading you through two steps.
- For faster setup, you can select **Add Auto-Discovery Group...** in the [context menu](#)²⁴⁷ of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.

 You cannot use this feature on the **Hosted Probe** of a PRTG hosted by Paessler instance. You can use this feature on [remote probes](#)³⁷⁰⁹.

- i** This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Add Auto-Discovery Group to Group Local Probe
✕

Create a group of monitoring objects that you want to explore with the help of PRTG's auto-discovery. Specify your group settings, the sensor management, a discovery schedule, the IP range for discovery, and the credentials for Windows, Linux, VMware/Xen, and SNMP, if necessary.

Help: Auto-Discovery

Group Name and Tags

Group Name: ⓘ

Group

Tags ⓘ

+

Group Type

Sensor Management ⓘ

Automatic device identification (standard, recommended)

Automatic device identification (detailed, may create many sensors)

Automatic sensor creation using specific device template(s)

Discovery Schedule

Once ▼

IP Selection Method

Class C base IP with start/end (IPv4)

List of individual IPs and DNS names (IPv4)

IP and subnet (IPv4)

IP with octet range (IPv4)

List of individual IPs and DNS names (IPv6)

Use computers from the active directory (maximum 1000 computers)

IPv4 Base

This field is required.

Cancel
Continue >

Add Auto-Discovery Group Dialog

- **Step 1**
Choose a probe or group you want to add the new group to. Click **Continue**.
- **Step 2**
Add auto-discovery settings as described below.

Add Auto-Discovery Group Settings

GROUP NAME AND TAGS

- Group Name** Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
- Tags** Enter one or more tags. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically [inherited](#) 139.

GROUP TYPE

- Sensor Management** Select the method for automatic network discovery. Choose between:
- **Automatic device identification (standard, recommended):** Detect mainly based on Ping, SNMP, and WMI. This option works fine for most installations.
 - **Automatic device identification (detailed, may create many sensors):** Detect in a more detailed way and create more sensors. This option uses all standard device templates for auto-discovery. It is suitable for small network segments and whenever you want to monitor the maximum number of sensors available.
 - **Automatic sensor creation using specific device template(s):** Manually define the device templates used for auto-discovery. From the list below, select one or more templates.

- Device Template(s)** This option is only visible if you enable using specific device templates above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. PRTG will use the selected templates for auto-discovery on the current device. Choose from:
- **ADSL**
 - **Amazon Cloudwatch**
 - **Buffalo TeraStation NAS**
 - **Cisco ASA VPN**
 - **Cisco Device (Generic)**

- **Dell EqualLogic**
- **Dell MDI Disk**
- **DNS Server**
- **Environment Jacarta**
- **Environment Poseidon**
- **FTP Server**
- **Generic Device (PING only)**
- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **IPMI enabled devices**
- **Juniper NS Device**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**
- **Mail Server (MS Exchange)**
- **Microsoft SharePoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**
- **Printer (HP)**
- **Printer Generic**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Server Cisco UCS**
- **Server IBM**
- **SonicWall**
- **SSL Security Check**
- **Switch (Cisco Catalyst)**

- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS Health (APC)**
- **UPS Health (Generic)**
- **UPS Health (Liebert)**
- **VMware ESX / vCenter Server**
- **Webserver**
- **Windows (Detailed via WMI)**
- **Windows (via Remote PowerShell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**
- **XEN Virtual Machines**

Once the auto-discovery is finished, PRTG will create a new [ticket](#) [230] and list the device templates that it used to create new sensors. The ticket will not show templates that were not applied.

Discovery Schedule

Define when PRTG will run the auto-discovery. Choose between:

- **Once:** Perform auto-discovery only once. PRTG will add new devices and sensors once. If you select this option, you have to [start the auto-discovery manually](#) [283], it will not run automatically.
 - **Hourly:** Perform auto-discovery for new devices and sensors every 60 minutes.
 - ⓘ Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour.
 - **Daily:** Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the [System Administration—Monitoring](#) [336] settings.
 - **Weekly:** Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the [System Administration—Monitoring](#) [336] settings.
- ⓘ The **Discovery Schedule** will be set to **Once** on all devices created by the scheduled auto-discovery for performance reasons.

IP Selection Method	<p>Define how you want to define the IP range for auto-discovery. Choose between:</p> <ul style="list-style-type: none"> ▪ Class C base IP with start/end (IPv4): Define an IPv4 class C address range. ▪ List of individual IPs and DNS names (IPv4): Enter a list of individual IPv4 addresses or DNS names. ▪ IP and subnet (IPv4): Enter an IPv4 address and subnet mask. ▪ IP with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ List of individual IPs and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names. ▪ Use computers from the active directory (maximum 1000 computers): Search in the active directory for computers to perform auto-discovery. <ul style="list-style-type: none"> ❗ Define your active directory domain in advance in the system administration. See System Administration—Core & Probes³³⁷². <p>❗ Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.</p>
IPv4 Base	<p>This field is only visible if you select Class C network detection above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, 192.168.0</p>
IPv4 Range Start	<p>This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 1 to discover from 192.168.0.1.</p>
IPv4 Range End	<p>This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 254 to discover up to 192.168.0.254.</p>
IPv4/DNS Name List IPv6/DNS Name List	<p>This field is only visible if you select the IP list option above. Enter a list of IP addresses or DNS names that the auto-discovery will scan. Enter each address in a separate line.</p>

IPv4 and Subnet (IPv4)	<p>This field is only visible if you select the IP and subnet option above. Enter an expression in the format address/subnet, for example, 192.168.3.0/255.255.255.0. You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.</p>
IP with Octet Range	<p>This field is only visible if you select the octet range option above. Enter an expression in the format a1.a2.a3.a4, where a1, a2, a3, and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127. All permutations of all ranges are calculated. For example, 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.</p>
Organizational Unit	<p>This field is only visible if you select active directory above. Enter an organizational unit (OU) to restrict the active directory search to computers that are part of this OU. Just enter the name of the OU without any other term (so without "OU" in front). If you leave this field empty, there will not be any restriction.</p> <p> Make sure that the OU contains a host. If the OU is empty, you will receive an error message.</p> <p>If you have sub-OUs, consider the correct syntax in the format Y,OU=X: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ Assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X ▪ For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X <p> The order is important, sub-OUs have to be listed left of their particular parents!</p>
Name Resolution	<p>Define how to monitor newly discovered devices. This affects only new devices. The setting for existing devices will remain unchanged. Depending on your selection the IP Address/DNS Name field of an added device^[402] shows the DNS name or IP address that PRTG uses to access the target device. Choose between:</p> <ul style="list-style-type: none"> ▪ Use DNS names (recommended): Monitor newly discovered devices via their DNS names (if available). ▪ Use IP addresses: Monitor newly discovered devices via their IP addresses. <p>We recommend that you use the default value.</p> <p> This setting does not affect how PRTG shows the devices in the device tree.</p>

Device Rescan

Define if you want to add devices that already exist in your PRTG installation also to the currently selected group. Choose between:

- **Skip auto-discovery for known devices/IPs (recommended):** Do not re-scan known devices or IP addresses, only add devices with new IPs or DNS names when auto-discovering. PRTG will not add devices that are already included elsewhere in your configuration, for example, in other groups.
- **Perform auto-discovery for known devices/IPs:** Re-scan devices with known IP addresses with every auto-discovery. This option will add devices that already exist in other groups also to this group and runs the auto-discovery on the newly added devices.
 - ❗ The auto-discovery will not run on devices that already exist in this group. If you want to run the auto-discovery for an existing device, you have to start the auto-discovery on this device.

We recommend that you use the default value.

- ❗ In certain cases, the IP resolution may not work and might result in a device not being added if it has the same local IP address as in another LAN.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

If you have not set credentials yet, set them now before starting the auto-discovery to fully exploit the power of this feature!

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Domain or Computer Name

Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do **not** leave this field empty.

CREDENTIALS FOR WINDOWS SYSTEMS

User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. <ul style="list-style-type: none">  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p> If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	<p>This setting is only visible if you enable manual port selection above. Enter the WBEM port number.</p>
SSH Port	<p>Enter the port number to use for SSH connections.</p> <p> By default, PRTG uses this setting automatically for all SSH sensors⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none"> ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above. ▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.
Target User	<p>This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.</p>
Password Target User	<p>This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.</p>

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Engine

Select the method you want to use to [access data with SSH sensors](#)³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Default (recommended):** This is the default monitoring method for SSH sensors. It provides best performance and security.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

 You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User

Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.

Password

Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.

 Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.

VMware Protocol

Define the protocol used for the connection to VMware and XenServer. Choose between:

- **HTTPS (recommended):** Use an SSL-encrypted connection to VMware and XenServers.
- **HTTP:** Use an unencrypted connection to VMware and XenServers.

Session Pool

Define if you want to use session pooling for VMware sensors. Choose between:

CREDENTIALS FOR VMWARE/XENSERVER

- **Reuse session for for multiple scans (recommended):** Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.
- **Create a new session for each scan:** If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#)⁴⁶³
- [Microsoft SQL v2 Sensor](#)¹²⁶⁷
- [MySQL v2 Sensor](#)¹²⁸⁴
- [Oracle SQL v2 Sensor](#)¹⁴⁵⁷
- [PostgreSQL Sensor](#)¹⁵⁷⁴

Port for Databases

Define which ports PRTG will use for connections to the monitored databases. Choose between:

- **Set automatically (default port, recommended):** PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors:** Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- **Microsoft SQL:** 1433

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **MySQL:** 3306
- **Oracle SQL:** 1521
- **PostgreSQL:** 5432

Custom Database Port	<p>Enter the number of the port that PRTG will use for database connections. Please enter an integer value.</p> <p> All database sensors on this device will use this port to connect.</p>
Authentication Mode	<p>Select the authentication method for the connection to the SQL database. Choose between:</p> <ul style="list-style-type: none">▪ Windows authentication with impersonation: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings^[407] for the database connection.  The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.▪ SQL server authentication: Choose this option if you want to use explicit credentials for database connections.
User	<p>This field is only visible if you select SQL server authentication above. Enter the username for the database connection.</p>
Password	<p>This field is only visible if you select SQL server authentication above. Enter the password for the database connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).</p>

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

CREDENTIALS FOR AMAZON CLOUDWATCH

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none"> ▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. <ul style="list-style-type: none"> ❗ SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP. ▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. <ul style="list-style-type: none"> ❗ When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the Probe Health Sensor^[159], distribute the load over multiple probes^[370]. SNMP v1 and v2 do not have this limitation.
Community String	This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

CREDENTIALS FOR SNMP DEVICES

Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none">▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication.▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <p>i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.</p>
User	<p>This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.</p>
Password	<p>This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.</p>
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p>i AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p>i The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p>i If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>

CREDENTIALS FOR SNMP DEVICES

Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

HTTP Proxy Settings	<p>The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.</p> <ul style="list-style-type: none">  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see System Administration—Core & Probes^[336].  The SSL Certificate Sensor^[263] and the SSL Security Check Sensor^[264] do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	<p>If the proxy requires authentication, enter the username for the proxy login.</p> <ul style="list-style-type: none">  Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

-  Only basic authentication is available! Please enter a string or leave the field empty.

ACCESS RIGHTS

User Group Access Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
- **Read:** Users in this group can see the object and review its settings.
- **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the [System Administration—User Groups](#) settings.

Save your settings. If you leave the current page, all changes to the settings will be lost!

Auto-Discovery in Progress

While auto-discovery is running you may experience a lower system performance as usual, because PRTG works in the background to discover your network. Depending on the IP ranges defined (up to 65,536 addresses), the discovery may run up to several days before it is complete. You can review the status of the discovery process as follows:

- In the device tree, behind the group or device name, you will see a percentage value showing the progress of auto-discovery.
- During auto-discovery, the web interface will display a box in the lower-right corner that shows the number of active auto-discovery tasks.
- To stop a running auto-discovery, right-click the group or device, and select **Pause | For 5 minutes...** from the [context menu](#). PRTG will [pause](#) monitoring for 5 minutes and stop auto-discovery tasks.

Disable Initial Auto-Discovery

To disable the initial auto-discovery for a fresh PRTG installation, simply run the installer in command prompt and add `/NoInitialAutoDisco=1` as parameter. This may be useful for performance reasons or if you prefer to manually add devices and sensors to your installation.

Related Topics

- [Create Device Template](#) 

More

Knowledge Base: Why can automatic auto-discoveries evoke performance issues?

- <https://kb.paessler.com/en/topic/14423>

Knowledge Base: How can I turn off Auto Discovery?

- <https://kb.paessler.com/en/topic/10403>

7.2 Create Objects Manually

We recommend that you use the [auto-discovery](#)^[282] function to create a basic monitoring setup for your network. Afterwards, you can manually create devices that could not be discovered, or [arrange](#)^[319] detected devices in groups.

The procedure depends on the kind of object you want to add. Choose between:

- [Add a Group](#)^[302]
- [Add a Device](#)^[311]
- [Add a Sensor](#)^[325]

Add a Remote Probe

 See section [Multiple Probes and Remote Probes](#)^[370] for more information.

7.2.1 Add a Group

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

There are several ways to add a group manually:

- Select **Devices | Add Group** from the main menu. An assistant will appear, leading you through two steps.
- Hover over  and select **Add Group** from the menu. An assistant will appear, leading you through two steps.
- For faster setup, you can select **Add Group...** in the [context menu](#)^[247] of a probe or group to which you want to add the new group. This will skip step 1 and lead you directly to step 2.
- **Step 1**
Choose a probe or group you want to add the new group to. Click **Continue**.

Add Group to Group Local Probe ✕

Define Group Settings

Choose a name for the group and—if desired—the Windows, Linux, VMware, and SNMP credential settings. These will be inherited to all devices in this group.

Help: [Add a Group](#)

Add a New Group

In PRTG your network devices are organized into groups. You can define as many groups as you like and you can create multiple levels of sub-groups.

Group Name and Tags

Group Name: ⓘ

Group

Tags

+

Credentials for Windows Systems

inherit from  Local Probe (Domain or Computer Name: paesslergmbh, User: ...)

Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems

inherit from  Local Probe (User: <empty>, Login: 0, For WBEM Use Port: 0...)

Credentials for VMware/XenServer

inherit from  Local Probe (User: <empty>)

Credentials for SNMP Devices

inherit from  Local Probe (SNMP Version: V2, SNMP Port: 161, SNMP Timeou...)

[Cancel](#)

Add Group Assistant Step 2

- **Step 2**
Add group settings as described below.

Add Group Settings

GROUP NAME AND TAGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more tags. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited ¹³⁹ .

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) ¹³⁷ for more information.

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) ¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
------	--

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. <ul style="list-style-type: none"> ❗ PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	<p>This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.</p>
Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p>❗ If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	<p>This setting is only visible if you enable manual port selection above. Enter the WBEM port number.</p>
SSH Port	<p>Enter the port number to use for SSH connections.</p> <p>❗ By default, PRTG uses this setting automatically for all SSH sensors⁴³⁴, unless you define a different port number in the sensor settings.</p>

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none">▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above.▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.
Target User	<p>This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.</p>
Password Target User	<p>This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.</p>
SSH Engine	<p>Select the method you want to use to access data with SSH sensors. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none">▪ Default (recommended): This is the default monitoring method for SSH sensors. It provides best performance and security.▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. <p> You can also individually select the SSH engine for each SSH sensor in the sensor settings.</p>

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.  Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: <ul style="list-style-type: none">▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers.▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: <ul style="list-style-type: none">▪ Reuse session for for multiple scans (recommended): Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.▪ Create a new session for each scan: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	Select the SNMP version for the device connection. Choose between:
--------------	--

CREDENTIALS FOR SNMP DEVICES

- **v1:** Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

i SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP.

- **v2c (recommended):** Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.

- **v3:** Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

i When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased **Interval Delay** or **Open Requests** with the **Probe Health Sensor**, distribute the load over **multiple probes**. SNMP v1 and v2 do not have this limitation.

Community String	This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <p>i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.</p>
User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.

CREDENTIALS FOR SNMP DEVICES

Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
- **Read:** Users in this group can see the object and review its settings.
- **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the [System Administration—User Groups](#) settings.

Save your settings. If you leave the current page, all changes to the settings will be lost!

7.2.2 Add a Device

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

There are several ways to add a device manually:

- Select **Devices | Add Device** from the main menu. An assistant will appear, leading you through two steps.
- Hover over  and select **Add Device** from the menu. An assistant will appear, leading you through two steps.
- For faster setup, you can select **Add Device...** in the [context menu](#)²⁴⁷ of a group to which you want to add the new device. This will skip step 1 and lead you directly to step 2.
- **Step 1**
Choose a group you want to add the new device to. Click **OK**.

Part 7: Ajax Web Interface—Device and Sensor Setup | 2 Create Objects Manually
 2 Add a Device

Add Device to Group Local Probe
✕

Add a New Device

Define a device name and address, options for auto-discovery, and credential settings for Windows, Linux, VMware/XEN, and SNMP, if necessary.

Help: Add a Device

Device Name and Address

Device Name ⓘ

IP Version ⓘ

Connect using IPv4

Connect using IPv6

IPv4 Address/DNS Name ⓘ

This field is required.

Tags ⓘ

+

Device Icon ⓘ

Device Type

Sensor Management ⓘ

Cancel
OK

Add Device Assistant Step 2

- **Step 2**
 Add device settings as described below.

Add Device Settings

DEVICE NAME AND ADDRESS

Device Name	Enter a meaningful name to identify the device. The name will be shown by default in the device tree and in all alarms.
IP Version	Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between: <ul style="list-style-type: none">▪ Connect using IPv4: Use IP version 4 for all requests to this device.▪ Connect using IPv6: Use IP version 6 for all requests to this device.
IP Address/DNS Name	Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors created on this device will inherit this setting and they will try to connect to this address for monitoring.  There are some sensor types that still have their own setting for IP address/DNS name. Those sensors will use their own settings.
Tags	Enter one or more tags; confirm each tag by hitting the space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. Tags are automatically inherited ¹³⁹ .
Device Icon	Choose a device icon from the list. It will be shown in the device tree.

DEVICE TYPE

Sensor Management	Select which type of auto-discovery you would like to perform for this device. Choose between: <ul style="list-style-type: none">▪ Manual (no auto-discovery): Select this if you want to only create sensors manually.▪ Automatic device identification (standard, recommended): Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device.
-------------------	--

DEVICE TYPE

- **Automatic device identification (detailed, may create many sensors):** Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device.
- **Automatic sensor creation using specific device template (s):** Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.

Discovery Schedule

This option is only visible if you select one of the auto-discovery options above. Define when the auto-discovery will run. Choose between:

- **Once:** Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. If you select this option, you have to [start the auto-discovery manually](#)^[283], it will not run automatically.
- **Hourly:** Perform auto-discovery for new sensors every hour.
- **Daily:** Perform auto-discovery for new sensors every day.
- **Weekly:** Perform auto-discovery for new sensors every week.

Device Template(s)

This option is only visible if using specific device templates (last option) is enabled above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from:

- **ADSL**
- **Amazon Cloudwatch**
- **Buffalo TeraStation NAS**
- **Cisco ASA VPN**
- **Cisco Device (Generic)**
- **Dell EqualLogic**
- **Dell MDI Disk**
- **DNS Server**
- **Environment Jakarta**
- **Environment Poseidon**
- **FTP Server**
- **Generic Device (PING only)**

DEVICE TYPE

- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **IPMI enabled devices**
- **Juniper NS Device**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**
- **Mail Server (MS Exchange)**
- **Microsoft SharePoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**
- **Printer (HP)**
- **Printer Generic**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Server Cisco UCS**
- **Server IBM**
- **SonicWall**
- **SSL Security Check**
- **Switch (Cisco Catalyst)**
- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS Health (APC)**
- **UPS Health (Generic)**

DEVICE TYPE

- **UPS Health (Liebert)**
- **VMware ESX / vCenter Server**
- **Webserver**
- **Windows (Detailed via WMI)**
- **Windows (via Remote PowerShell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**
- **XEN Virtual Machines**

Once the auto-discovery is finished, PRTG will create a new [ticket](#) ^[230] and list the device templates that were actually used to create new sensors. Templates that were not applied will not be shown in the ticket.

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) ^[137] for more information.

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. <ul style="list-style-type: none">  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p> If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Port	<p>Enter the port number to use for SSH connections.</p> <p> By default, PRTG uses this setting automatically for all SSH sensors ⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none">▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above.▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.
Target User	<p>This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.</p>
Password Target User	<p>This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.</p>
SSH Engine	<p>Select the method you want to use to access data with SSH sensors ³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none">▪ Default (recommended): This is the default monitoring method for SSH sensors. It provides best performance and security.▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

-  You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.  Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: <ul style="list-style-type: none">▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers.▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: <ul style="list-style-type: none">▪ Reuse session for for multiple scans (recommended): Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.▪ Create a new session for each scan: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none"> ▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. <ul style="list-style-type: none">  SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP. ▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. <ul style="list-style-type: none">  When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the Probe Health Sensor¹⁵⁹⁰, distribute the load over multiple probes³⁷⁰⁹. SNMP v1 and v2 do not have this limitation.
Community String	<p>This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.</p>
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <ul style="list-style-type: none">  If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

CREDENTIALS FOR SNMP DEVICES

User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) ¹³⁷ for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#) ⁴⁶³
- [Microsoft SQL v2 Sensor](#) ¹²⁶⁷
- [MySQL v2 Sensor](#) ¹²⁸⁴
- [Oracle SQL v2 Sensor](#) ¹⁴⁵⁷
- [PostgreSQL Sensor](#) ¹⁵⁷⁴

Port for Databases Define which ports PRTG will use for connections to the monitored databases. Choose between:

- **Set automatically (default port, recommended):** PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors:** Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- **Microsoft SQL:** 1433
- **MySQL:** 3306
- **Oracle SQL:** 1521
- **PostgreSQL:** 5432

Custom Database Port Enter the number of the port that PRTG will use for database connections. Please enter an integer value.

 All database sensors on this device will use this port to connect.

Authentication Mode Select the authentication method for the connection to the SQL database. Choose between:

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **Windows authentication with impersonation:** If you select this option, PRTG uses the Windows credentials as defined in the particular [device settings](#)^[407] for the database connection.
 - ❗ The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.
- **SQL server authentication:** Choose this option if you want to use explicit credentials for database connections.

User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Save your settings. If you leave the current page, all changes to the settings will be lost!

7.2.3 Add a Sensor

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

There are several ways to add a sensor manually:

- Select **Sensors | Add Sensor** from the main menu. An assistant will appear, leading you through two steps.
- Hover over  and select **Add Sensor** from the menu. An assistant will appear, leading you through two steps.
- For faster setup, you can select **Add Sensor...** in the [context menu](#)²⁴⁷ of a device to which you want to add the new sensor. This will skip step 1 and lead you directly to [step 2](#)³²⁷.
- You can also click the **Add Sensor** button at the end of a device's sensor list on the device tree screen or above the Geo Map on the right.

Step 1 - Select Device

Add Sensor

< Cancel sensor creation

Choose a Device to Add the New Sensor to

Create a new device

Add sensor to an existing device

Select a Group from the List

Select a device from the list. Tip: You can create new sensors much faster by right clicking a device and choosing Add Sensor from the context menu. Continue >

Search...

- Root
 - Local Probe
 - Probe Device
 - Network Discovery
 - Network Infrastructure
 - Internet
 - Gateway
 - DHCP
 - Exchange
 - ADS
 - DNS/ADS
 - DNS
 - Windows
 - Clients
 - nue-ph

This field is required.

Add Sensor Dialog

- Select **Add sensor to an existing device** (default setting).
- Choose the device you want to add the new sensor to.
- Click **Continue**.

The add sensor assistant appears.

Step 2 - Choose Sensor Type

The add sensor assistant helps you choose the correct sensor (see screenshot above).

- Narrow down the sensor types:
 - Choose appropriate criteria to filter the shown sensor types. **A**
 - Enter (parts of) the name into the search box. **B**
 - Go through the detailed list of sensors matching the selected device. **C**
 - If you cannot find a suitable sensor, search for custom sensors in our PRTG Script World. Just click **Looking For More Sensor Types?** below the list of sensor types. See section [List of Available Sensor Types—Script World Sensors](#) ^[450].
- Choose which sensor best monitors the parameters you require.
- Click the sensor box to select this sensor.

The sensor settings dialog opens.

- Enter suitable sensor settings.

-  PRTG suggests sensor types to create on the selected device. This recommendation is automatically calculated based on the current user's sensor usage and shows the ten most commonly used sensor types (if enough sensor types are already in use).
-  If you are unsure which sensor type will provide the information you require, then we recommend that you use the filter categories to progressively narrow down your choices.

You can either:

- Select the type of parameter you want to monitor via **Monitor What?**. 
 - Specify the type of target system you want to monitor and see what sensors are available for this type of hardware in **Target System Type?**. 
 - Choose the technology that you want to use for monitoring (for example SNMP or WMI) in **Technology Used?**. 
-  Please also consider whether a sensor's performance impact is high or low by checking the bar in the lower left corner of the sensor box. For further information, see this Knowledge Base article: [How to Speed Up PRTG](#) (especially section 4 - Sensor Type and Monitoring Considerations)
- Confirm by clicking **Create**.

PRTG will now create the sensor. The device tree opens.

-  For more information about a sensor type, see the manual section of the respective sensor (directly accessible via the question mark (?) symbol in the top-right corner). You can also go to the [List of Available Sensor Types](#) ⁴²⁹ section to find a comprehensive overview of sensor types.

More

Knowledge Base: How can I change the number of entries in most used sensor types?

- <https://kb.paessler.com/en/topic/59788>

Knowledge Base: How to Speed Up PRTG (especially section 4 - Sensor Type and Monitoring Considerations)

- <https://kb.paessler.com/en/topic/2733>

7.3 Manage Device Tree

While viewing the device tree (or parts of it), click the **Management** tab to enter a different tree view that shows your devices and sensors in a less colorful way. While in this view, you can move monitoring objects using **drag&drop** in your browser window. You can also view and edit object settings by selecting the object. Changes take effect immediately. When done, leave the **Management** tab.

To arrange objects in the tree, you have the following options:

Drag&Drop a Sensor

You can either move a sensor within the same device, or clone a sensor to another device.

- Within the same device, drag any sensor and drop it to the place where you want to have it. A shadow will show the future position. When dropping, the sensor will be **moved** to this position and existing sensors will be lined up after it. This is a very easy way to reposition your sensors.
- Drag any sensor from one device and drop it on another to **clone** a sensor. This will create the same sensor type, with the same settings, on the new device, while maintaining the original sensor. A shade will show the future position.
 - ❶ Cloned sensors are put to **Pause** status initially to give you the chance to change any settings before monitoring begins. Please check the [settings](#)^[217] and [resume](#)^[245] monitoring.
- ❶ You cannot clone **fixed** objects, such as the root group, a probe device, or PRTG system internal sensors.
- ❶ To **clone** entire groups or devices, please use the [Clone Object](#)^[3193] functionality accessible via the objects' [Context Menu](#)^[247].

Drag&Drop a Group or Device

You can change a group's or device's position by using drag&drop.

- Within the same probe or group, drag any group or device and move it up or down in the device tree. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to this position and existing probes, groups, and devices will be lined up underneath. This is a very easy way to reposition your groups or devices.
- Drag any group or device from one probe or group and drop it on another probe or group. A small red arrow will appear, showing the future position. When dropping, the group or device will be moved to the new probe or group. Existing groups and devices will be lined up underneath. This is a very easy way to change the probe a group or device is part of, or to add groups or devices to other groups.
- ❶ You cannot move the **Local Probe**, **Hosted Probe** and **Remote Probes**.

Multi-Edit Object Properties

You can use Multi-Edit for object settings:

- Hold down the **Ctrl** key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you want to edit, change the according values, and click **Save**. The changes will be applied to all selected objects.

The dialog is the same as described in the [Multi-Edit](#)³¹⁹⁹ (Edit Settings) section.

Related Topics

For other ways to arrange objects, see

- [Arrange Objects](#)³¹⁹¹
- [Create Device Template](#)³²⁰³
- [Clone Object](#)³¹⁹³

7.4 Root Group Settings

On the **Root** group's overview page, click the **Settings** tab to change settings.

The Root Group is Special

The **Root** group is the highest instance in the object hierarchy of your PRTG setup and parent to all other objects. Therefore, all objects inherit settings from the **Root** group. If you define important settings on this high level, work will be easier later on. So, before you create your own sensors, it is a good idea to review the **Root** group's settings to ensure they suit your network. There are already reasonable presets made with installation.

i If necessary, you can override every setting for every single child object later. To do so, simply disable the respective **Inherit** option of an object.

Root Group Settings

The following settings are available in the **Settings** tab. As you may not need all of these, just regard the settings you really need and ignore the others. All settings you define here can easily be inherited to all other objects in your setup.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC GROUP SETTINGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Define if monitoring for this group is started or paused. Choose between: <ul style="list-style-type: none">▪ Started: Monitor this group.▪ Paused: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.

LOCATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Location (for Geo Maps)

When you want to use [Geo Maps](#)^[3211], enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the [sensor status icons](#)^[195] (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: **49.452778 11.077778** or **enter 49.452778 any 11.077778 text**

A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map.

 The preview map will always have a road map layout regardless of the map layout you set in [User Interface](#)^[3346].

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Domain or Computer Name

Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do **not** leave this field empty.

User

Enter the username for Windows access. Usually, you will use credentials with administrator privileges.

Password

Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. <ul style="list-style-type: none">  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p> If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Port	<p>Enter the port number to use for SSH connections.</p> <p> By default, PRTG uses this setting automatically for all SSH sensors ⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none">▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above.▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.
Target User	<p>This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.</p>
Password Target User	<p>This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.</p>
SSH Engine	<p>Select the method you want to use to access data with SSH sensors ³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none">▪ Default (recommended): This is the default monitoring method for SSH sensors. It provides best performance and security.▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

-  You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.  Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: <ul style="list-style-type: none">▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers.▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: <ul style="list-style-type: none">▪ Reuse session for for multiple scans (recommended): Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.▪ Create a new session for each scan: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none"> ▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. <ul style="list-style-type: none">  SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP. ▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. <ul style="list-style-type: none">  When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the Probe Health Sensor¹⁵⁹⁰, distribute the load over multiple probes³⁷⁰⁹. SNMP v1 and v2 do not have this limitation.
Community String	<p>This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.</p>
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <p> If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.</p>

CREDENTIALS FOR SNMP DEVICES

User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)  for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#) 
- [Microsoft SQL v2 Sensor](#) 
- [MySQL v2 Sensor](#) 
- [Oracle SQL v2 Sensor](#) 
- [PostgreSQL Sensor](#) 

Port for Databases Define which ports PRTG will use for connections to the monitored databases. Choose between:

- **Set automatically (default port, recommended):** PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors:** Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- **Microsoft SQL:** 1433
- **MySQL:** 3306
- **Oracle SQL:** 1521
- **PostgreSQL:** 5432

Custom Database Port Enter the number of the port that PRTG will use for database connections. Please enter an integer value.

 All database sensors on this device will use this port to connect.

Authentication Mode Select the authentication method for the connection to the SQL database. Choose between:

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **Windows authentication with impersonation:** If you select this option, PRTG uses the Windows credentials as defined in the particular [device settings](#)^[407] for the database connection.
 - ❗ The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.
- **SQL server authentication:** Choose this option if you want to use explicit credentials for database connections.

User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for troubleshooting.

Preferred Data Source	<p>Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between:</p> <ul style="list-style-type: none"> ▪ Performance Counters and fallback to WMI: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only (recommended): Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	<p>Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:</p> <ul style="list-style-type: none"> ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. <p>We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.</p>
Timeout Value (Sec.)	<p>This field is only visible if the manual timeout method is selected above. Enter the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

SNMP COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for troubleshooting.

SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100 , higher delays are not supported and will be discarded.
Failed Requests	<p>Define if an SNMP sensor will try again after a request fails.</p> <ul style="list-style-type: none">▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	<p>Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore overflow values: Ignore overflow values and do not include them in the monitoring data.▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. <p>We recommend that you use the default value.</p> <p> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option Ignore overflow values in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?</p>
Zero Values	<p>Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data.▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. <p>We recommend that you use the default value. If you experience problems, change this option.</p>

SNMP COMPATIBILITY OPTIONS

- 32-bit/64-bit Counters** Define which kind of traffic counters PRTG will search for on a device.
- **Use 64-bit counters if available (recommended):** The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.
 - **Use 32-bit counters only:** The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices.

We recommend that you use the default value. If you experience problems, change this option.

- Request Mode** Define which kind of request method PRTG uses for SNMP sensors.
- **Use multi get (recommended):** Bundle multiple SNMP requests into one request.
 - **Use single get:** Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

 PRTG uses **paging** for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

- Port Name Template** Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as **(001) Ethernet1**, for example. You can use any field names available at a certain OID of your device, among which are:
- **[port]:** The port number of the monitored interface.
 - **[ifalias]:** The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
 - **[ifname]:** The textual name of the monitored interface as assigned by the local device.
 - **[ifdescr]:** A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.

SNMP COMPATIBILITY OPTIONS

- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]**: The type of the sensor, this is **SNMP Traffic** or **SNMP RMON**. This is useful to differentiate between your [SNMP Traffic](#) ²⁴⁶⁷ and [SNMP RMON](#) ²⁴⁰⁵ sensors.

Combine them as you like to obtain suitable sensor names.

 For more information about SNMP sensor names, see this Knowledge Base article: [How can I change the defaults for names automatically generated for new SNMP sensors?](#)

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

 For more information about automatic updates of names, see this Knowledge Base article: [Automatically update port name and number for SNMP Traffic sensors when the device changes them](#)

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
 -  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
 -  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
 -  When using this option, it is important that your device returns unique interface names in the ifName field.

SNMP COMPATIBILITY OPTIONS

- **No Port Update:** Use this option to disable automatic port identification.

Start Interface Index For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will start to query the interface range during sensor creation. Use **0** for automatic mode. We recommend that you use the default value.

End Interface Index For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will stop to query the interface range during sensor creation. Use **0** for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ⓘ If a channel uses [lookup](#)^[3693] values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Schedule Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the [account settings](#)^[331].

- ⓘ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window Specify if you want to set-up a one-time maintenance window. During a maintenance window, this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

- ⓘ To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency settings are available only in [Probe Settings](#)^[351], [Group Settings](#)^[375], [Device Settings](#)^[402], and [Sensor Settings](#)^[428].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Unusual Detection Define if you want to benefit from [unusual detection](#)^[336] for sensors. You can configure the behavior of unusual detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate unusual detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. Sensors affected by this setting will turn to orange color ([unusual sensor status](#)^[195]) if PRTG detects unusual activity.
- **Disabled:** Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensors will not show an unusual sensor status.

Similar Sensors Detection Define if you want to activate [Similar Sensors](#)^[209] analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate similar sensors detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. PRTG considers all sensors affected by this setting during similarity analysis.

ADVANCED NETWORK ANALYSIS

- System Information
- **Disabled:** Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
- Define if you want to retrieve and show [System Information](#)^[222] for your devices. Choose between:
- **Enabled:** Activate the system information feature for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree.
 - **Disabled:** Do not activate system information.
-  **System Information** is enabled by default. To retrieve the data, PRTG will automatically use **Credentials for Windows Systems** and **Credentials for SNMP Devices** as defined in the [device settings](#)^[402] or as [inherited](#)^[133] from a parent object like the **Root** group. Please consider this when you monitor devices outside the local network, especially when using **SNMP v1** or **v2c** that do not provide encryption.
-  This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, see [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see [Object Settings](#)^[217] section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <https://kb.paessler.com/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

7.5 Probe Settings

On a probe's overview page, click the **Settings** tab to change settings.

Add Remote Probe

You can add additional remote probes to your setup to extend your monitoring to networks that are not directly reachable by your PRTG core installation or cluster.

 See section [Add Remote Probe](#)^[3707] for more details.

Probe Settings

The following settings are available in the **Settings** tab of every probe. Because you may not need all of these for every probe, just regard the settings you really need, ignoring the others.

We recommend that you define as many settings as possible in the **Root**^[331] group, so you can inherit them to all other objects further down in the [device tree hierarchy](#)^[133].

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC PROBE SETTINGS

Probe Name	Enter a meaningful name to identify the probe. The name will be shown by default in the devices tree and in all alarms.
Tags	Enter one or more Tags ^[139] . Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
Status	Choose if monitoring for this probe is started or paused. <ul style="list-style-type: none"> ▪ Started: Monitor this probe. ▪ Paused: Pause monitoring for this probe. All sensors on all devices on this probe will be paused until this setting is changed again.

BASIC PROBE SETTINGS

Priority Select a priority for the probe. This setting determines where the probe will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

LOCATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Location (for Geo Maps) When you want to use [Geo Maps](#)³²¹, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the [sensor status icons](#)¹⁹⁵ (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: **49.452778 11.077778** or **enter 49.452778 any 11.077778 text**

A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map.

 The preview map will always have a road map layout regardless of the map layout you set in [User Interface](#)^{334b}.

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	Define the authentication method to use for login. Choose between: <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication.  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p>i If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	<p>This setting is only visible if you enable manual port selection above. Enter the WBEM port number.</p>
SSH Port	<p>Enter the port number to use for SSH connections.</p> <p>i By default, PRTG uses this setting automatically for all SSH sensors⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none"> ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above. ▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

- **Run the command as another user using 'su':** Use the rights of another user with **su** to run commands on the target device.

Target User This field is only visible if you choose **sudo** or **su** above. Enter a username to run the specified command as a user other than **root**. If you leave this field empty, you will run the command as **root**. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.

Password Target User This field is only visible if you choose to run the commands using **su** or **sudo** with password above. Enter the password for the specified target user.

SSH Engine Select the method you want to use to [access data with SSH sensors](#)³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Default (recommended):** This is the default monitoring method for SSH sensors. It provides best performance and security.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

 You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷¹ for more information.

User Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.

Password Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.

-  Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.

CREDENTIALS FOR VMWARE/XENSERVER

VMware Protocol	<p>Define the protocol used for the connection to VMware and XenServer. Choose between:</p> <ul style="list-style-type: none">▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers.▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Session Pool	<p>Define if you want to use session pooling for VMware sensors. Choose between:</p> <ul style="list-style-type: none">▪ Reuse session for for multiple scans (recommended): Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.▪ Create a new session for each scan: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none">▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.  SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP.▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.
--------------	--

CREDENTIALS FOR SNMP DEVICES

i When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased **Interval Delay** or **Open Requests** with the **Probe Health Sensor**, distribute the load over **multiple probes**. SNMP v1 and v2 do not have this limitation.

Community String This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5:** Use **Message-Digest Algorithm 5** (MD5) for authentication.
- **SHA:** Use **Secure Hash Algorithm** (SHA) for authentication.

The type you choose must match the authentication type of your device.

i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, **SNMP_SEC_LEVEL_NOAUTH** is used and authentication deactivated entirely.

User This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES:** Use **Data Encryption Standard** (DES) as encryption algorithm.
- **AES:** Use **Advanced Encryption Standard** (AES) as encryption algorithm.

i AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.

CREDENTIALS FOR SNMP DEVICES

 The type that you choose must match the encryption type of your device.

Data Encryption Key

This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.

 If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.

Context Name

This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.

SNMP Port

Enter the port for the SNMP communication. We recommend that you use the default value.

SNMP Timeout (Sec.)

Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is **300** seconds (5 minutes).

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#)^[463]
- [Microsoft SQL v2 Sensor](#)^[1267]
- [MySQL v2 Sensor](#)^[1284]
- [Oracle SQL v2 Sensor](#)^[1457]
- [PostgreSQL Sensor](#)^[1574]

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Port for Databases	<p>Define which ports PRTG will use for connections to the monitored databases. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (default port, recommended): PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ Define one custom port valid for all database sensors: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. <p>If you choose the automatic port selection, PRTG uses the following default ports:</p> <ul style="list-style-type: none"> ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	<p>Enter the number of the port that PRTG will use for database connections. Please enter an integer value.</p> <p> All database sensors on this device will use this port to connect.</p>
Authentication Mode	<p>Select the authentication method for the connection to the SQL database. Choose between:</p> <ul style="list-style-type: none"> ▪ Windows authentication with impersonation: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings^[407] for the database connection. <ul style="list-style-type: none">  The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ SQL server authentication: Choose this option if you want to use explicit credentials for database connections.
User	<p>This field is only visible if you select SQL server authentication above. Enter the username for the database connection.</p>
Password	<p>This field is only visible if you select SQL server authentication above. Enter the password for the database connection.</p>

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Timeout (Sec.) Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is **300** seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Access Key Enter your Amazon Web Services (AWS) access key. Please see the corresponding [Amazon CloudWatch sensor](#)^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

Secret Key Enter your Amazon Web Services (AWS) secret key. Please see the corresponding [Amazon CloudWatch sensor](#)^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for troubleshooting.

Preferred Data Source Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between:

- **Performance Counters and fallback to WMI:** Try to query data via performance counters. If this is not possible, establish a connection via WMI.
- **Performance Counters only:** Query data via performance counters only. If this is not possible, a sensor will return no data.

WINDOWS COMPATIBILITY OPTIONS

- **WMI only (recommended):** Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.

Timeout Method Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:

- **Use 1.5x scanning interval (recommended):** Use a default of one and a half times the scanning interval set for the sensor (see below in this settings).
- **Set manually:** Enter a timeout value manually.

We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.

Timeout Value (Sec.) This field is only visible if the manual timeout method is selected above. Enter the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

SNMP COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for troubleshooting.

SNMP Delay (ms) Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between **0** and **100**, higher delays are not supported and will be discarded.

Failed Requests Define if an SNMP sensor will try again after a request fails.

- **Retry (recommended):** Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.

SNMP COMPATIBILITY OPTIONS

	<ul style="list-style-type: none">▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	<p>Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore overflow values: Ignore overflow values and do not include them in the monitoring data.▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. <p>We recommend that you use the default value.</p> <p> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option Ignore overflow values in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?</p>
Zero Values	<p>Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data.▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. <p>We recommend that you use the default value. If you experience problems, change this option.</p>
32-bit/64-bit Counters	<p>Define which kind of traffic counters PRTG will search for on a device.</p> <ul style="list-style-type: none">▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. <p>We recommend that you use the default value. If you experience problems, change this option.</p>
Request Mode	<p>Define which kind of request method PRTG uses for SNMP sensors.</p>

SNMP COMPATIBILITY OPTIONS

- **Use multi get (recommended):** Bundle multiple SNMP requests into one request.
- **Use single get:** Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

 PRTG uses **paging** for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **[port] [ifalias]** is set as port name template, which will create a name such as **(001) Ethernet1**, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]:** The port number of the monitored interface.
- **[ifalias]:** The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]:** The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]:** A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]:** An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]:** The type of the sensor, this is **SNMP Traffic** or **SNMP RMON**. This is useful to differentiate between your **SNMP Traffic** [2467] and **SNMP RMON** [2405] sensors.

Combine them as you like to obtain suitable sensor names.

 For more information about SNMP sensor names, see this Knowledge Base article: [How can I change the defaults for names automatically generated for new SNMP sensors?](#)

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

SNMP COMPATIBILITY OPTIONS

- **Keep port names (use this if you edit the names in PRTG):** Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device:** If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

 For more information about automatic updates of names, see this Knowledge Base article: [Automatically update port name and number for SNMP Traffic sensors when the device changes them](#)

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended):** Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
 -  ifName will not be tried automatically.
- **Use ifAlias:** For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr:** Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
 -  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName:** You can also use this option if there is no unique ifAlias available.
 -  When using this option, it is important that your device returns unique interface names in the ifName field.
- **No Port Update:** Use this option to disable automatic port identification.

Start Interface Index

For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

End Interface Index

For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Distribution This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will **not** be included in sensor scans. By default, this setting is [inherited](#)¹³⁷ to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the [account settings](#)³³¹.

 Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

 To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. <p> You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule.</p> <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[240] to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	<p>This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay.</p> <p>After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Unusual Detection Define if you want to benefit from [unusual detection](#)^[336] for sensors. You can configure the behavior of unusual detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate unusual detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. Sensors affected by this setting will turn to orange color ([unusual sensor status](#)^[195]) if PRTG detects unusual activity.
- **Disabled:** Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensors will not show an unusual sensor status.

Similar Sensors Detection Define if you want to activate [Similar Sensors](#)^[209] analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate similar sensors detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. PRTG considers all sensors affected by this setting during similarity analysis.

ADVANCED NETWORK ANALYSIS

System Information

- **Disabled:** Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.

Define if you want to retrieve and show [System Information](#)^[222] for your devices. Choose between:

- **Enabled:** Activate the system information feature for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree.
- **Disabled:** Do not activate system information.

 **System Information** is enabled by default. To retrieve the data, PRTG will automatically use **Credentials for Windows Systems** and **Credentials for SNMP Devices** as defined in the [device settings](#)^[402] or as [inherited](#)^[133] from a parent object like the **Root** group. Please consider this when you monitor devices outside the local network, especially when using **SNMP v1** or **v2c** that do not provide encryption.

 This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

 This feature does not support all sensor types for technical reasons.

 If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

PROBE SETTINGS FOR MONITORING

Outgoing IPv4 Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

Outgoing IPv6 Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

 For details about the basic concept of IPv6 in PRTG, see the [IPv6](#) section.

Cluster Connectivity This box is only visible if you run a PRTG cluster. Define if this probe connects to all cluster nodes, including the failover nodes, or only to the primary master node. Choose between:

- **Probe sends data only to primary master node:** The probe connects only to the primary master node. You are not able to review monitoring data on failover nodes. Consider choosing this option if you have bandwidth limitations in your network or if the probe cannot access your failover node(s).
- **Probe sends data to all cluster nodes:** This is the default option. The probe connects to all nodes in your cluster and sends monitoring data to the failover node(s) in addition to the primary master. The probe is visible on all your nodes as soon as it connects automatically to the correct IP addresses and ports of the failover nodes. If your master node fails, you can still see monitoring data of this probe.

 PRTG will not notify you if a remote probe is disconnected from a cluster node. Please check explicitly on a cluster node if your remote probes are connected (for example, via the device tree in the PRTG web interface on a cluster node).

SCHEDULED RESTART SETTINGS

 This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Restart Options For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options:

SCHEDULED RESTART SETTINGS

- **No scheduled reboot or service restart:** Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under [System Administration—Administrative Tools](#) in the PRTG web interface.
- **Scheduled restart of PRTG services:** Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below.
- **Scheduled system reboot (recommended):** We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.

Restart Schedule

You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server:

- **Once per week:** Select a day of the week and a time below.
- **Once per month (recommended):** Select a day of the month and a time below.

Specify Day

You can only see this setting if you selected a schedule option above. Select a specific day of the week (**Monday** to **Sunday**) or month (**1st** to **30th** or **Last**). If you select **Last**, the restart will always be executed on the last day of the month, regardless of how many days the month has.

 If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.

Specify Hour

You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart.

 You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, see [Sensor Notification Triggers Settings](#) ³¹⁷⁰ section.

Others

For more general information about settings, see [Object Settings](#) ²¹⁷¹ section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <https://kb.paessler.com/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

7.6 Group Settings

On a group's overview page, click the **Settings** tab to change settings.

Add Group

The **Add Group** dialog appears when adding a new group to a parent group. It only shows the setting fields that are imperative for creating the group. Therefore, you will not see all setting fields in this dialog. For example, the **Group Status** option is not available in this step.

You can change all settings in the group's **Settings** tab later.

Group Settings

The following settings are available in the **Settings** tab of every group. As you may not need all of these for every group, just regard the settings you really need, ignoring the others.

i This documentation does not refer to the setting of the special **Root** group. The settings available there differ from those described here.

We recommend that you define as many settings as possible in the **Root** group, so you can inherit them to all other objects further down in the [device tree hierarchy](#).

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC GROUP SETTINGS

Group Name	Enter a meaningful name to identify the group. The name will be shown by default in the devices tree and in all alarms.
Status	Choose if monitoring for this group is started or paused. We recommend that you use the default value. You can add additional tags to it, if you like. <ul style="list-style-type: none"> ▪ Started: Monitor this group. ▪ Paused: Pause monitoring for this group. All sensors on all devices in this group will be paused until this setting is changed again.
Parent Tags	Shows Tags that this group inherits from its parent probe . This setting is shown for your information only and cannot be changed here.

BASIC GROUP SETTINGS

Tags Enter one or more [Tags](#)¹³⁹. Confirm each tag by hitting the space, comma, or enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case sensitive.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the group. This setting determines where the group will be placed in list views. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).

GROUP TYPE

Sensor Management Select which type of auto-discovery you would like to perform for this group. Choose between:

- **Manual (no auto-discovery):** Do not auto-discover any sensors, only add sensors manually.
- **Automatic device identification (standard, recommended):** Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device.
- **Automatic device identification (detailed, may create many sensors):** Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device.
- **Automatic sensor creation using specific device templates:** Use specific auto-discovery templates only. Select templates below. This will scan your LAN and add sensors defined in the template.

Device Template(s) This option is only visible if you enable using specific device templates above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. PRTG will use the selected templates for auto-discovery on the current device. Choose from:

- **ADSL**
- **Amazon Cloudwatch**

- **Buffalo TeraStation NAS**
- **Cisco ASA VPN**
- **Cisco Device (Generic)**
- **Dell EqualLogic**
- **Dell MDI Disk**
- **DNS Server**
- **Environment Jakarta**
- **Environment Poseidon**
- **FTP Server**
- **Generic Device (PING only)**
- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **IPMI enabled devices**
- **Juniper NS Device**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**
- **Mail Server (MS Exchange)**
- **Microsoft SharePoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**
- **Printer (HP)**
- **Printer Generic**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Server Cisco UCS**
- **Server IBM**

- SonicWall
- SSL Security Check
- Switch (Cisco Catalyst)
- Switch (Cisco IOS Based)
- Switch (HP Procurve)
- UNIX/Linux Device
- UPS Health (APC)
- UPS Health (Generic)
- UPS Health (Liebert)
- VMware ESX / vCenter Server
- Webserver
- Windows (Detailed via WMI)
- Windows (via Remote PowerShell)
- Windows (via WMI)
- Windows IIS (via SNMP)
- XEN Hosts
- XEN Virtual Machines

Once the auto-discovery is finished, PRTG will create a new [ticket](#) ^[230] and list the device templates that it used to create new sensors. The ticket will not show templates that were not applied.

Discovery Schedule

Define when PRTG will run the auto-discovery. Choose between:

- **Once:** Perform auto-discovery only once. PRTG will add new devices and sensors once. If you select this option, you have to [start the auto-discovery manually](#) ^[283], it will not run automatically.
- **Hourly:** Perform auto-discovery for new devices and sensors every 60 minutes.
 - ⓘ Please use this option with caution! Frequently executed auto-discoveries might cause performance issues, especially when large network segments are scanned every hour.
- **Daily:** Perform auto-discovery for new devices and sensors every 24 hours. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the **Auto-Discovery Settings** section of the [System Administration—Monitoring](#) ^[330] settings.

	<ul style="list-style-type: none"> ▪ Weekly: Perform auto-discovery for new devices and sensors every 7 days. The first auto-discovery will run immediately, all other discoveries will start at the time defined in the Auto-Discovery Settings section of the System Administration—Monitoring settings. <p>i The Discovery Schedule will be set to Once on all devices created by the scheduled auto-discovery for performance reasons.</p>
IP Selection Method	<p>Define how you want to define the IP range for auto-discovery. Choose between:</p> <ul style="list-style-type: none"> ▪ Class C base IP with start/end (IPv4): Define an IPv4 class C address range. ▪ List of individual IPs and DNS names (IPv4): Enter a list of individual IPv4 addresses or DNS names. ▪ IP and subnet (IPv4): Enter an IPv4 address and subnet mask. ▪ IP with octet range (IPv4): Enter an IPv4 address range for every IP octet individually. With this, you can define very customizable IP ranges. ▪ List of individual IPs and DNS names (IPv6): Enter a list of individual IPv6 addresses or DNS names. ▪ Use computers from the active directory (maximum 1000 computers): Search in the active directory for computers to perform auto-discovery. <ul style="list-style-type: none"> i Define your active directory domain in advance in the system administration. See System Administration—Core & Probes. <p>i Only subnets with up to 65,536 IP addresses can be discovered! If you define a range with a higher number of addresses, discovery will stop before it is completed.</p>
IPv4 Base	<p>This field is only visible if you select Class C network detection above. Enter a class C network as IP base for the auto-discovery. Enter the first three octets of an IPv4 IP address, for example, 192.168.0</p>
IPv4 Range Start	<p>This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above from which PRTG will start the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 1 to discover from 192.168.0.1.</p>
IPv4 Range End	<p>This field is only visible if you select Class C network detection above. Enter the IP octet of the class C network specified above at which PRTG will stop the auto-discovery. This will complete the IP base above to an IPv4 address. For example, enter 254 to discover up to 192.168.0.254.</p>

IPv4/DNS Name List IPv6/DNS Name List	This field is only visible if you select the IP list option above. Enter a list of IP addresses or DNS names that the auto-discovery will scan. Enter each address in a separate line.
IPv4 and Subnet (IPv4)	This field is only visible if you select the IP and subnet option above. Enter an expression in the format address/subnet , for example, 192.168.3.0/255.255.255.0 . You can also use the short form like 192.168.3.0/24 in this example. PRTG will scan the complete host range (without network and broadcast address) defined by the IP address and the subnet mask.
IP with Octet Range	This field is only visible if you select the octet range option above. Enter an expression in the format a1.a2.a3.a4 , where a1 , a2 , a3 , and a4 are each a number between 0-255, or a range with two numbers and a hyphen like 1-127 . All permutations of all ranges are calculated. For example, 10.0.1-10.1-100 results in 1,000 addresses that PRTG will scan during auto-discovery.
Organizational Unit	<p>This field is only visible if you select active directory above. Enter an organizational unit (OU) to restrict the active directory search to computers that are part of this OU. Just enter the name of the OU without any other term (so without "OU" in front). If you leave this field empty, there will not be any restriction.</p> <p> Make sure that the OU contains a host. If the OU is empty, you will receive an error message.</p> <p>If you have sub-OUs, consider the correct syntax in the format Y,OU=X: OUs that are part of another OU have to be listed together with their parent(s). Enter the sub-OU followed by ,OU= and the name of the parent OU.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ Assuming that the organizational unit 'Y' is part of the OU named 'X'. Then the syntax would be Y,OU=X ▪ For three OUs 'X', 'Y' part of 'X', and 'Z' part of 'Y', the syntax would be Z,OU=Y,OU=X <p> The order is important, sub-OUs have to be listed left of their particular parents!</p>
Name Resolution	<p>Define how to monitor newly discovered devices. This affects only new devices. The setting for existing devices will remain unchanged. Depending on your selection the IP Address/DNS Name field of an added device^[402] shows the DNS name or IP address that PRTG uses to access the target device. Choose between:</p> <ul style="list-style-type: none"> ▪ Use DNS names (recommended): Monitor newly discovered devices via their DNS names (if available). ▪ Use IP addresses: Monitor newly discovered devices via their IP addresses.

We recommend that you use the default value.

-  This setting does not affect how PRTG shows the devices in the device tree.

Device Rescan

Define if you want to add devices that already exist in your PRTG installation also to the currently selected group. Choose between:

- **Skip auto-discovery for known devices/IPs (recommended):** Do not re-scan known devices or IP addresses, only add devices with new IPs or DNS names when auto-discovering. PRTG will not add devices that are already included elsewhere in your configuration, for example, in other groups.
- **Perform auto-discovery for known devices/IPs:** Re-scan devices with known IP addresses with every auto-discovery. This option will add devices that already exist in other groups also to this group and runs the auto-discovery on the newly added devices.
 -  The auto-discovery will not run on devices that already exist in this group. If you want to run the auto-discovery for an existing device, you have to start the auto-discovery on this device.

We recommend that you use the default value.

-  In certain cases, the IP resolution may not work and might result in a device not being added if it has the same local IP address as in another LAN.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

LOCATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

LOCATION

Location (for Geo Maps)

When you want to use [Geo Maps](#)³²¹¹, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the [sensor status icons](#)¹⁹⁵¹ (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: **49.452778 11.077778** or **enter 49.452778 any 11.077778 text**

A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map.

 The preview map will always have a road map layout regardless of the map layout you set in [User Interface](#)³³⁴⁶.

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷¹ for more information.

Domain or Computer Name

Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do **not** leave this field empty.

User

Enter the username for Windows access. Usually, you will use credentials with administrator privileges.

Password

Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication. <ul style="list-style-type: none">  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	<p>This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.</p> <p> If you do not insert a private key for the first time, but change the private key, you need to restart your PRTG core server service³³⁸⁸ in order for the private key change to take effect! For details, see Monitoring via SSH³⁵¹⁰.</p>
For WBEM Use Protocol	<p>Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	<p>Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

SSH Port	<p>Enter the port number to use for SSH connections.</p> <p> By default, PRTG uses this setting automatically for all SSH sensors ⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	<p>Define the rights that you want to use to execute the command on the target system. Choose between:</p> <ul style="list-style-type: none">▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above.▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user.▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.
Target User	<p>This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root. If you leave this field empty, you will run the command as root. Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.</p>
Password Target User	<p>This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.</p>
SSH Engine	<p>Select the method you want to use to access data with SSH sensors ³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none">▪ Default (recommended): This is the default monitoring method for SSH sensors. It provides best performance and security.▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

-  You can also individually select the SSH engine for each SSH sensor in the sensor settings.

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.  Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between: <ul style="list-style-type: none">▪ HTTPS (recommended): Use an SSL-encrypted connection to VMware and XenServers.▪ HTTP: Use an unencrypted connection to VMware and XenServers.
Session Pool	Define if you want to use session pooling for VMware sensors. Choose between: <ul style="list-style-type: none">▪ Reuse session for for multiple scans (recommended): Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.▪ Create a new session for each scan: If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none"> ▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. <ul style="list-style-type: none">  SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP. ▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. <ul style="list-style-type: none">  When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the Probe Health Sensor¹⁵⁰⁰, distribute the load over multiple probes³⁷⁰⁹. SNMP v1 and v2 do not have this limitation.
Community String	<p>This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.</p>
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <ul style="list-style-type: none">  If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.

CREDENTIALS FOR SNMP DEVICES

User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.
Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#)⁴⁶³
- [Microsoft SQL v2 Sensor](#)¹²⁶⁷
- [MySQL v2 Sensor](#)¹²⁸⁴
- [Oracle SQL v2 Sensor](#)¹⁴⁵⁷
- [PostgreSQL Sensor](#)¹⁵⁷⁴

Port for Databases Define which ports PRTG will use for connections to the monitored databases. Choose between:

- **Set automatically (default port, recommended):** PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports.
- **Define one custom port valid for all database sensors:** Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors.

If you choose the automatic port selection, PRTG uses the following default ports:

- **Microsoft SQL:** 1433
- **MySQL:** 3306
- **Oracle SQL:** 1521
- **PostgreSQL:** 5432

Custom Database Port Enter the number of the port that PRTG will use for database connections. Please enter an integer value.

 All database sensors on this device will use this port to connect.

Authentication Mode Select the authentication method for the connection to the SQL database. Choose between:

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

- **Windows authentication with impersonation:** If you select this option, PRTG uses the Windows credentials as defined in the particular [device settings](#)^[407] for the database connection.
 - ❗ The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation.
- **SQL server authentication:** Choose this option if you want to use explicit credentials for database connections.

User	This field is only visible if you select SQL server authentication above. Enter the username for the database connection.
Password	This field is only visible if you select SQL server authentication above. Enter the password for the database connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is 300 seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Access Key	Enter your Amazon Web Services (AWS) access key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.
Secret Key	Enter your Amazon Web Services (AWS) secret key. Please see the corresponding Amazon CloudWatch sensor ^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for troubleshooting.

Preferred Data Source	<p>Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between:</p> <ul style="list-style-type: none"> ▪ Performance Counters and fallback to WMI: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ Performance Counters only: Query data via performance counters only. If this is not possible, a sensor will return no data. ▪ WMI only (recommended): Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	<p>Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:</p> <ul style="list-style-type: none"> ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. <p>We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.</p>
Timeout Value (Sec.)	<p>This field is only visible if the manual timeout method is selected above. Enter the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

SNMP COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP COMPATIBILITY OPTIONS

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for troubleshooting.

SNMP Delay (ms)	Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100 , higher delays are not supported and will be discarded.
Failed Requests	Define if an SNMP sensor will try again after a request fails. <ul style="list-style-type: none">▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks. <ul style="list-style-type: none">▪ Ignore overflow values: Ignore overflow values and do not include them in the monitoring data.▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. We recommend that you use the default value. <p> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option Ignore overflow values in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?</p>
Zero Values	Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks. <ul style="list-style-type: none">▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data.▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. We recommend that you use the default value. If you experience problems, change this option.

SNMP COMPATIBILITY OPTIONS

- 32-bit/64-bit Counters** Define which kind of traffic counters PRTG will search for on a device.
- **Use 64-bit counters if available (recommended):** The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.
 - **Use 32-bit counters only:** The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices.

We recommend that you use the default value. If you experience problems, change this option.

- Request Mode** Define which kind of request method PRTG uses for SNMP sensors.
- **Use multi get (recommended):** Bundle multiple SNMP requests into one request.
 - **Use single get:** Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

 PRTG uses **paging** for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

- Port Name Template** Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **([port]) [ifalias]** is set as port name template, which will create a name such as **(001) Ethernet1**, for example. You can use any field names available at a certain OID of your device, among which are:
- **[port]:** The port number of the monitored interface.
 - **[ifalias]:** The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
 - **[ifname]:** The textual name of the monitored interface as assigned by the local device.
 - **[ifdescr]:** A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.

SNMP COMPATIBILITY OPTIONS

- **[ifspeed]**: An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]**: The type of the sensor, this is **SNMP Traffic** or **SNMP RMON**. This is useful to differentiate between your [SNMP Traffic](#) ²⁴⁶⁷ and [SNMP RMON](#) ²⁴⁰⁵ sensors.

Combine them as you like to obtain suitable sensor names.

 For more information about SNMP sensor names, see this Knowledge Base article: [How can I change the defaults for names automatically generated for new SNMP sensors?](#)

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

- **Keep port names (use this if you edit the names in PRTG)**: Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device**: If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

 For more information about automatic updates of names, see this Knowledge Base article: [Automatically update port name and number for SNMP Traffic sensors when the device changes them](#)

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended)**: Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
 -  ifName will not be tried automatically.
- **Use ifAlias**: For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr**: Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
 -  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName**: You can also use this option if there is no unique ifAlias available.
 -  When using this option, it is important that your device returns unique interface names in the ifName field.

SNMP COMPATIBILITY OPTIONS

- **No Port Update:** Use this option to disable automatic port identification.

Start Interface Index For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will start to query the interface range during sensor creation. Use **0** for automatic mode. We recommend that you use the default value.

End Interface Index For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will stop to query the interface range during sensor creation. Use **0** for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Distribution This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will **not** be included in sensor scans. By default, this setting is [inherited](#)¹³⁷ to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. <p>i You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule.</p> <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects should be paused. You can check all dependencies^[3209] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[240] to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	<p>This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay.</p> <p>After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Unusual Detection Define if you want to benefit from [unusual detection](#)^[336] for sensors. You can configure the behavior of unusual detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate unusual detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. Sensors affected by this setting will turn to orange color ([unusual sensor status](#)^[195]) if PRTG detects unusual activity.
- **Disabled:** Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensors will not show an unusual sensor status.

Similar Sensors Detection Define if you want to activate [Similar Sensors](#)^[209] analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate similar sensors detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. PRTG considers all sensors affected by this setting during similarity analysis.

ADVANCED NETWORK ANALYSIS

- **Disabled:** Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
- System Information Define if you want to retrieve and show [System Information](#)^[222] for your devices. Choose between:
- **Enabled:** Activate the system information feature for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree.
 - **Disabled:** Do not activate system information.
-  **System Information** is enabled by default. To retrieve the data, PRTG will automatically use **Credentials for Windows Systems** and **Credentials for SNMP Devices** as defined in the [device settings](#)^[402] or as [inherited](#)^[133] from a parent object like the **Root** group. Please consider this when you monitor devices outside the local network, especially when using **SNMP v1** or **v2c** that do not provide encryption.
-  This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

NUMBER OF SENSORS LIMITATION

- Sensor Limit This setting allows the administrator to set a limit for the maximum number of sensors in this group. Subgroups are also included in this limitation. If the amount of sensors exceeds the limitation, surplus sensors will be [paused](#)^[245]. This is of special interest for a Managed Service Provider (MSP). Choose between:
- **Allow unlimited number of sensors:** Do not limit the number of sensors for this group. Any number of sensors can be added to this group and its subgroups.
 - **Limit number of sensors in this group:** Enable a limitation for the number of sensors in this group. Only a defined number of sensors can monitor in this group and its subgroups.
- Maximum Number of Sensors This field is only visible if you enable limitation above. Define how many sensors are allowed in this group and its subgroups. Sensors that exceed this group sensor limit will be paused. Please enter an integer value.

NUMBER OF SENSORS LIMITATION

- ❗ Sensors in [paused status](#)^[195] count for this group limit as well (for example, manually paused sensors, sensors paused by dependency or schedule), but not for the number of available sensors in your license.
- ❗ Manually paused sensors will override the sensor message "exceeds group sensor limit".

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, see [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see [Object Settings](#)^[2171] section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <https://kb.paessler.com/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

7.7 Device Settings

On the details page of a device, click the **Settings** tab to change settings.

Add Device

The **Add Device** dialog appears when you add a new device to a group. It only shows the setting fields that are imperative for creating the device in PRTG. Because of this, you will not see all setting fields in this dialog. For example, the **Device Status** option is not available in this step.

 You can change all settings in the **Settings** tab of the device later.

Device Settings

The following settings are available in the **Settings** tab of every device. Because you do not need all of these for every device, depending on the device type, just define the settings you really need and ignore the others.

We recommend that you define as many settings as possible in the [Root](#) ³³¹ group, so you can inherit them to all other objects further down in the [device tree hierarchy](#) ¹³³.

For device settings, there is also multi-edit available. This enables you to change the properties of many devices at a time.

 For more details, see [Multi-Edit Lists](#) ³¹⁹⁷ section.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC DEVICE SETTINGS

Device Name	Enter a meaningful name to identify the device. PRTG shows this name by default in the device tree ¹⁸¹ and in all Alarms ²¹⁹ and Notifications ³²¹⁶ .
Status	Define the activity status of the device. Choose between: <ul style="list-style-type: none"> ▪ Started: Monitor this device. ▪ Paused: Pause monitoring for this device. All sensors on it are in status ¹⁹⁵ Paused until you change this setting again.

BASIC DEVICE SETTINGS

IP Version	<p>Define which IP protocol PRTG will use to connect to this device. The setting is valid for all sensors created on this device. Choose between:</p> <ul style="list-style-type: none"> ▪ IPv4 device: Use IP version 4 for all requests to this device. ▪ IPv6 device: Use IP version 6 for all requests to this device.
IP Address/DNS Name	<p>Enter the IP address (either v4 or v6, depending on your selection above) or DNS name for the device. Most sensors you create on this device will inherit this setting and try connecting to this address for monitoring.</p> <p> Some sensor types have their own setting for IP address/DNS name to which they connect.</p>
Parent Tags	<p>Shows Tags^[139] that this device inherits^[140] from its parent group and probe^[133]. This setting is shown for your information only and cannot be changed here.</p>
Tags	<p>Enter one or more Tags^[139]. Confirm each tag by with the space, comma, or enter key. Sensors on this device inherit these tags. You can use tags to group sensors and tag-filtered views, for example, in Libraries^[325]. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags, if you like.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority^[242] for the device. This setting determines the order in which your devices are displayed when you view table lists. Top priority will be at the top of a list. You can choose from one star (low priority) to five stars (top priority).</p>

ADDITIONAL DEVICE INFORMATION

Device Icon	Choose a device icon from the list. PRTG shows it in the device tree.
-------------	---

ADDITIONAL DEVICE INFORMATION

 For information on how to add your custom icons to PRTG on premises instances, see this article in the Knowledge Base: [How can I add my own device icons for use in the PRTG web interface?](#)

Service URL

Specify a URL you would like to open directly when you select **Device Tools | Go To Service URL** from the [context menu](#)^[254] of the device. For example, you can configure this option to call the address <http://www.example.com/service.html>. Enter a valid URL or leave the field empty.

DEVICE TYPE

Sensor Management

Select which type of auto-discovery you would like to perform for this device. Choose between:

- **Manual (no auto-discovery):** Select this if you want to only create sensors manually.
- **Automatic device identification (standard, recommended):** Use a small set of auto-discovery templates. This will scan your LAN and usually create a set of standard sensors on your device.
- **Automatic device identification (detailed, may create many sensors):** Use an extended set of auto-discovery templates. This will scan your LAN and usually create many sensors on your device.
- **Automatic sensor creation using specific device template (s):** Use specific auto-discovery templates only. Please select templates below. This will scan your LAN and add sensors defined in the template.

Discovery Schedule

This option is only visible if you select one of the auto-discovery options above. Define when the auto-discovery will run. Choose between:

- **Once:** Perform auto-discovery only once. For existing devices, this will initiate a one-time sensor update for the current device. If you select this option, you have to [start the auto-discovery manually](#)^[283], it will not run automatically.
- **Hourly:** Perform auto-discovery for new sensors every hour.
- **Daily:** Perform auto-discovery for new sensors every day.
- **Weekly:** Perform auto-discovery for new sensors every week.

DEVICE TYPE

Device Template(s) This option is only visible if using specific device templates (last option) is enabled above. Choose one or more templates by adding a check mark in front of the respective template name. You can also select and deselect all items by using the check box in the table head. These will be used for auto-discovery on the current device. Choose from:

- **ADSL**
- **Amazon Cloudwatch**
- **Buffalo TeraStation NAS**
- **Cisco ASA VPN**
- **Cisco Device (Generic)**
- **Dell EqualLogic**
- **Dell MDI Disk**
- **DNS Server**
- **Environment Jakarta**
- **Environment Poseidon**
- **FTP Server**
- **Generic Device (PING only)**
- **Generic Device (SNMP-enabled)**
- **Generic Device (SNMP-enabled, Detailed)**
- **HTTP Web Server**
- **Hyper V Host Server**
- **IPMI enabled devices**
- **Juniper NS Device**
- **Linux/UNIX Device (SNMP or SSH enabled)**
- **Mail Server (Generic)**
- **Mail Server (MS Exchange)**
- **Microsoft SharePoint 2010**
- **NAS LenovoEMC**
- **NAS QNAP**
- **NAS Synology**
- **NetApp**
- **NTP Server**

DEVICE TYPE

- **Printer (HP)**
- **Printer Generic**
- **RDP Server**
- **RMON compatible device**
- **Server (Compaq/HP agents)**
- **Server (Dell)**
- **Server Cisco UCS**
- **Server IBM**
- **SonicWall**
- **SSL Security Check**
- **Switch (Cisco Catalyst)**
- **Switch (Cisco IOS Based)**
- **Switch (HP Procurve)**
- **UNIX/Linux Device**
- **UPS Health (APC)**
- **UPS Health (Generic)**
- **UPS Health (Liebert)**
- **VMware ESX / vCenter Server**
- **Webserver**
- **Windows (Detailed via WMI)**
- **Windows (via Remote PowerShell)**
- **Windows (via WMI)**
- **Windows IIS (via SNMP)**
- **XEN Hosts**
- **XEN Virtual Machines**

Once the auto-discovery is finished, PRTG will create a new [ticket](#) ^[230] and list the device templates that were actually used to create new sensors. Templates that were not applied will not be shown in the ticket.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

LOCATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Location (for Geo Maps)

When you want to use [Geo Maps](#)³²¹, enter a location in the first line. Geographical maps will display objects (devices, groups) then with a flag, showing the current status using a color code similar to the [sensor status icons](#)¹⁹⁵ (green - yellow - orange - red). You can enter a full postal address, city and country only, or latitude and longitude. It is possible to enter any text before, between, and after the coordinates, PRTG will parse latitude and longitude automatically, for example: **49.452778 11.077778** or **enter 49.452778 any 11.077778 text**

A minus sign (-) in the first line will hide an object from geo maps. In this case you can enter location information in line two and following.

You can define a specific label for each location: enter a string denoting the label in the first line and provide geo coordinates in the second line. This geo marker will show then the object with the label in the PRTG geo map.

 The preview map will always have a road map layout regardless of the map layout you set in [User Interface](#)³³⁴⁶.

CREDENTIALS FOR WINDOWS SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

CREDENTIALS FOR WINDOWS SYSTEMS

Domain or Computer Name	Define the authority for Windows access. This is used for Windows Management Instrumentation (WMI) and other Windows sensors. If you want to use a Windows local user account on the target device, enter the computer name here. If you want to use a Windows domain user account (recommended), enter the (Active Directory) domain name here. If not explicitly defined, PRTG will automatically add a prefix in order to use the NT LAN Manager (NTLM) protocol. Do not leave this field empty.
User	Enter the username for Windows access. Usually, you will use credentials with administrator privileges.
Password	Enter the password for Windows access. Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for the access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Login	<p>Define the authentication method to use for login. Choose between:</p> <ul style="list-style-type: none"> ▪ Login via Password: Provide a password for login. Enter below. ▪ Login via Private Key: Provide a private key for authentication.  PRTG can only handle keys in OpenSSH format that are not encrypted. You cannot use password-protected keys here. In the text field, paste the entire private key, including the "BEGIN" and "END" lines. Please make sure the according public key is provided on the target machine. For details, see Monitoring via SSH³⁵¹⁰.
Password	This field is only visible if you select password login above. Enter a password for the Linux access via SSH and WBEM. Usually, you will use credentials with administrator privileges.
Private Key	This field is only visible if you select private key login above. Paste a private key into the field (OpenSSH format, unencrypted). Usually, you will use credentials with administrator privileges.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

i If you do not insert a private key for the first time, but **change** the private key, you need to [restart your PRTG core server service](#)³³⁸⁸ in order for the private key change to take effect! For details, see [Monitoring via SSH](#)³⁵¹⁰.

For WBEM Use Protocol	Define the protocol to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: <ul style="list-style-type: none"> ▪ HTTP: Use an unencrypted connection for WBEM. ▪ HTTPS: Use an SSL-encrypted connection for WBEM.
For WBEM Use Port	Define the port to use for WBEM. This setting is only relevant if you use WBEM sensors. Choose between: <ul style="list-style-type: none"> ▪ Set automatically (port 5988 or 5989): Use one of the standard ports, depending on whether you choose unencrypted or encrypted connection above. ▪ Set manually: Use a custom port. Define below.
WBEM Port	This setting is only visible if you enable manual port selection above. Enter the WBEM port number.
SSH Port	Enter the port number to use for SSH connections. <p>i By default, PRTG uses this setting automatically for all SSH sensors⁴³⁴, unless you define a different port number in the sensor settings.</p>
SSH Rights Elevation	Define the rights that you want to use to execute the command on the target system. Choose between: <ul style="list-style-type: none"> ▪ Run the command as the user connecting (default): Use the rights of the user who establishes the SSH connection, as defined above. ▪ Run the command as another user using 'sudo' (with password): Use the rights of another user with a password required for sudo to run commands on the target device, for example, as root user. ▪ Run the command as another user using 'sudo' (without password): Use the rights of another user without a password required for sudo to run commands on the target device, for example, as root user. ▪ Run the command as another user using 'su': Use the rights of another user with su to run commands on the target device.

CREDENTIALS FOR LINUX/SOLARIS/MAC OS (SSH/WBEM) SYSTEMS

Target User	This field is only visible if you choose sudo or su above. Enter a username to run the specified command as a user other than root . If you leave this field empty, you will run the command as root . Ensure you set the Linux password even if you use a public or private key for authentication. This is not necessary if the user is allowed to execute the command without a password.
Password Target User	This field is only visible if you choose to run the commands using su or sudo with password above. Enter the password for the specified target user.
SSH Engine	<p>Select the method you want to use to access data with SSH sensors³⁵¹⁰. We strongly recommend that you keep the default engine! For now, you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none"> ▪ Default (recommended): This is the default monitoring method for SSH sensors. It provides best performance and security. ▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine. <p> You can also individually select the SSH engine for each SSH sensor in the sensor settings.</p>

CREDENTIALS FOR VMWARE/XENSERVER

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User	Enter a login name for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.
Password	<p>Enter a password for access to VMware and Xen servers. Usually, you will use credentials with administrator privileges.</p> <p> Single Sign-On (SSO) passwords for vSphere do not support special characters. See the manual sections for VMware sensors for details.</p>
VMware Protocol	Define the protocol used for the connection to VMware and XenServer. Choose between:

CREDENTIALS FOR VMWARE/XENSERVICES

- **HTTPS (recommended):** Use an SSL-encrypted connection to VMware and XenServers.
- **HTTP:** Use an unencrypted connection to VMware and XenServers.

Session Pool

Define if you want to use session pooling for VMware sensors. Choose between:

- **Reuse session for for multiple scans (recommended):** Select this option to use session pooling. With session pooling, a VMware sensor uses the same session as created in advance to query data and needs not to log in and out for each sensor scan. We recommend that you choose this option because it reduces network load and log entries on the target device, resulting in better performance.
- **Create a new session for each scan:** If you select this option and disable session pooling, a VMware sensor has to log in and out for each sensor scan. We recommend that you use the session pooling option above for better performance.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version

Select the SNMP version for the device connection. Choose between:

- **v1:** Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.
 -  **SNMP v1 does not support 64-bit counters.**
This may result in invalid data when monitoring traffic via SNMP.
- **v2c (recommended):** Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.
- **v3:** Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

CREDENTIALS FOR SNMP DEVICES

i When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased **Interval Delay** or **Open Requests** with the **Probe Health Sensor**, distribute the load over **multiple probes**. SNMP v1 and v2 do not have this limitation.

Community String This setting is only visible if you select SNMP version **v1** or **v2c** above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.

Authentication Type This setting is only visible if you select SNMP version **v3** above. Choose between:

- **MD5**: Use **Message-Digest Algorithm 5** (MD5) for authentication.
- **SHA**: Use **Secure Hash Algorithm** (SHA) for authentication.

The type you choose must match the authentication type of your device.

i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, **SNMP_SEC_LEVEL_NOAUTH** is used and authentication deactivated entirely.

User This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use **Data Encryption Standard** (DES) as encryption algorithm.
- **AES**: Use **Advanced Encryption Standard** (AES) as encryption algorithm.

i AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.

CREDENTIALS FOR SNMP DEVICES

 The type that you choose must match the encryption type of your device.

Data Encryption Key

This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.

 If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.

Context Name

This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.

SNMP Port

Enter the port for the SNMP communication. We recommend that you use the default value.

SNMP Timeout (Sec.)

Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is **300** seconds (5 minutes).

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

The settings you define in this section apply to the following sensor types:

- [ADO SQL v2 Sensor](#)⁴⁶³
- [Microsoft SQL v2 Sensor](#)¹²⁶⁷
- [MySQL v2 Sensor](#)¹²⁸⁴
- [Oracle SQL v2 Sensor](#)¹⁴⁵⁷
- [PostgreSQL Sensor](#)¹⁵⁷⁴

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Port for Databases	<p>Define which ports PRTG will use for connections to the monitored databases. Choose between:</p> <ul style="list-style-type: none"> ▪ Set automatically (default port, recommended): PRTG automatically determines the type of the monitored database and uses the corresponding default port to connect. See below for a list of default ports. ▪ Define one custom port valid for all database sensors: Choose this option if your database management systems do not use the default ports. Define the port for database connections manually below. If you choose this option, PRTG will use the custom port for all database sensors. <p>If you choose the automatic port selection, PRTG uses the following default ports:</p> <ul style="list-style-type: none"> ▪ Microsoft SQL: 1433 ▪ MySQL: 3306 ▪ Oracle SQL: 1521 ▪ PostgreSQL: 5432
Custom Database Port	<p>Enter the number of the port that PRTG will use for database connections. Please enter an integer value.</p> <p> All database sensors on this device will use this port to connect.</p>
Authentication Mode	<p>Select the authentication method for the connection to the SQL database. Choose between:</p> <ul style="list-style-type: none"> ▪ Windows authentication with impersonation: If you select this option, PRTG uses the Windows credentials as defined in the particular device settings^[407] for the database connection. <ul style="list-style-type: none">  The user whose credentials are used needs to have permissions to log on to the system on which the PRTG probe with a database sensor runs. This is required for the impersonation. ▪ SQL server authentication: Choose this option if you want to use explicit credentials for database connections.
User	<p>This field is only visible if you select SQL server authentication above. Enter the username for the database connection.</p>
Password	<p>This field is only visible if you select SQL server authentication above. Enter the password for the database connection.</p>

CREDENTIALS FOR DATABASE MANAGEMENT SYSTEMS

Timeout (Sec.) Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. The maximum timeout value is **300** seconds (5 minutes).

CREDENTIALS FOR AMAZON CLOUDWATCH

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Access Key Enter your Amazon Web Services (AWS) access key. Please see the corresponding [Amazon CloudWatch sensor](#)^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

Secret Key Enter your Amazon Web Services (AWS) secret key. Please see the corresponding [Amazon CloudWatch sensor](#)^[435] documentation to learn more about the rights that are required for querying AWS CloudWatch metrics.

WINDOWS COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

When experiencing problems while monitoring via Windows sensors, you can set some compatibility options for troubleshooting.

Preferred Data Source Define the method Windows sensors will use to query data. This setting is valid only for hybrid sensors offering performance counter and Windows Management Instrumentation (WMI) technology. The setting will be ignored for all other sensors! Choose between:

- **Performance Counters and fallback to WMI:** Try to query data via performance counters. If this is not possible, establish a connection via WMI.
- **Performance Counters only:** Query data via performance counters only. If this is not possible, a sensor will return no data.

WINDOWS COMPATIBILITY OPTIONS

	<ul style="list-style-type: none"> ▪ WMI only (recommended): Query data via WMI only. If this is not possible, a sensor will return no data. In current PRTG versions, this is our recommendation to achieve best performance and stability.
Timeout Method	<p>Specify the time the sensor will wait for the return of its WMI query before aborting it with an error message. Choose between:</p> <ul style="list-style-type: none"> ▪ Use 1.5x scanning interval (recommended): Use a default of one and a half times the scanning interval set for the sensor (see below in this settings). ▪ Set manually: Enter a timeout value manually. <p>We recommend that you use the default value. Only if you experience ongoing timeout errors, try increasing the timeout value.</p>
Timeout Value (Sec.)	<p>This field is only visible if the manual timeout method is selected above. Enter the time the sensor will wait for the return of its WMI query before aborting with an error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

SNMP COMPATIBILITY OPTIONS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

When experiencing problems while monitoring via Simple Network Management Protocol (SNMP) sensors, you can set some compatibility options for troubleshooting.

SNMP Delay (ms)	<p>Add a time in milliseconds that will be waited between two SNMP requests. This can help increase device compatibility. Please enter an integer value. We recommend that you use the default value. If you experience SNMP connection failures, please increase it. You can define a delay between 0 and 100, higher delays are not supported and will be discarded.</p>
Failed Requests	<p>Define if an SNMP sensor will try again after a request fails.</p> <ul style="list-style-type: none"> ▪ Retry (recommended): Try again if an SNMP request fails. This can help prevent false error messages due to temporary timeout failures.

SNMP COMPATIBILITY OPTIONS

	<ul style="list-style-type: none">▪ Do not retry: Do not retry if an SNMP request fails. With this setting enabled an SNMP sensor will be set to error status earlier.
Overflow Values	<p>Define how PRTG will handle overflow values. Some devices do not handle internal buffer overflows correctly. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore overflow values: Ignore overflow values and do not include them in the monitoring data.▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. <p>We recommend that you use the default value.</p> <p> If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the monitored device resets counters without an overflow. PRTG interprets such a behavior as overflow that results in data peaks. Choose the option Ignore overflow values in this case. For more details, see this Knowledge Base article: What is the Overflow Values setting in the SNMP Compatibility Options?</p>
Zero Values	<p>Define how PRTG will handle zero values. Some devices send incorrect zero values. This can cause false peaks.</p> <ul style="list-style-type: none">▪ Ignore zero values for delta sensors (recommended): Ignore zero values and do not include them in the monitoring data.▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data. <p>We recommend that you use the default value. If you experience problems, change this option.</p>
32-bit/64-bit Counters	<p>Define which kind of traffic counters PRTG will search for on a device.</p> <ul style="list-style-type: none">▪ Use 64-bit counters if available (recommended): The interface scan will use 64-bit traffic counters, if available. This can avoid buffer overflows in the devices.▪ Use 32-bit counters only: The interface scan will always use 32-bit traffic counters, even if 64-bit counters are available. This can lead to more reliable monitoring for some devices. <p>We recommend that you use the default value. If you experience problems, change this option.</p>
Request Mode	<p>Define which kind of request method PRTG uses for SNMP sensors.</p>

SNMP COMPATIBILITY OPTIONS

- **Use multi get (recommended):** Bundle multiple SNMP requests into one request.
- **Use single get:** Use one request for each SNMP value. This can increase compatibility with older devices.

We recommend that you use the default value. If you experience problems, change this option.

 PRTG uses **paging** for SNMP requests. This means that if a sensor has to query more than 20 OIDs, it will automatically poll the OIDs in packages of 20 OIDs each per request.

Port Name Template

Define how the name of SNMP sensors created on a device will be put together. Enter a template using several variables. When adding new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID usually several fields are available with interface descriptions. They are different for every device and OID. PRTG will use the information in these fields to name the sensors. If a field is empty or not available, an empty string is added to the name. As default, **[port] [ifalias]** is set as port name template, which will create a name such as **(001) Ethernet1**, for example. You can use any field names available at a certain OID of your device, among which are:

- **[port]:** The port number of the monitored interface.
- **[ifalias]:** The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling.
- **[ifname]:** The textual name of the monitored interface as assigned by the local device.
- **[ifdescr]:** A textual string containing information about the monitored device or interface, for example, manufacturer, product name, version.
- **[ifspeed]:** An estimate of the monitored interface's current bandwidth (KBit/s).
- **[ifsensor]:** The type of the sensor, this is **SNMP Traffic** or **SNMP RMON**. This is useful to differentiate between your **SNMP Traffic** [2467] and **SNMP RMON** [2405] sensors.

Combine them as you like to obtain suitable sensor names.

 For more information about SNMP sensor names, see this Knowledge Base article: [How can I change the defaults for names automatically generated for new SNMP sensors?](#)

Port Name Update

Define how PRTG will react if you change port names in your physical device (for example, a switch or router). Choose between:

SNMP COMPATIBILITY OPTIONS

- **Keep port names (use this if you edit the names in PRTG):** Do not automatically adjust sensor names. This is the best option if you want to change names in PRTG manually.
- **Automatic sensor name update if name changes in device:** If PRTG detects changes of port names in your physical device, it will try to automatically adjust sensor names accordingly.

 For more information about automatic updates of names, see this Knowledge Base article: [Automatically update port name and number for SNMP Traffic sensors when the device changes them](#)

Port Identification

Define which field will be used for SNMP interface identification. Choose between:

- **Automatic (recommended):** Tries the ifAlias field first to identify an SNMP interface and then ifDescr.
 -  ifName will not be tried automatically.
- **Use ifAlias:** For most devices ifAlias is the best field to get unique interface names.
- **Use ifDescr:** Use this option if the port order of your device changes after a reboot, and there is no ifAlias field available. For example, this is the best option for Cisco ASA devices.
 -  When using this option it is important that your device returns unique interface names in the ifDescr field.
- **Use ifName:** You can also use this option if there is no unique ifAlias available.
 -  When using this option, it is important that your device returns unique interface names in the ifName field.
- **No Port Update:** Use this option to disable automatic port identification.

Start Interface Index

For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will start to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

End Interface Index

For [SNMP Traffic sensors](#)²⁴⁶⁷, define at which index PRTG will stop to query the interface range during sensor creation. Use 0 for automatic mode. We recommend that you use the default value.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)^[3368].
-  The [SSL Certificate Sensor](#)^[2635] and the [SSL Security Check Sensor](#)^[2646] do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[3355] on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

CLUSTER USAGE

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Distribution This box is only visible if you run a PRTG cluster. Sometimes you want to exclude a certain node from monitoring the sensors running on this probe, group, or device, for example, if a device is not reachable from every node configured in your cluster. In the list of cluster nodes, please select the nodes that will **not** be included in sensor scans. By default, this setting is [inherited](#)¹³⁷ to all objects underneath.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted; the according settings from the parent objects will always be active. However, you can define additional settings here. They will be active in parallel to the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to pause monitoring for a certain time span (days, hours) throughout the week. You can create new schedules and edit existing ones in the [account settings](#)³³¹.

 Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active.

Maintenance Window Specify if you want to set-up a one-time maintenance window. During a maintenance window this object and all child objects will not be monitored. They will enter a paused state then. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window.

 To terminate a current maintenance window before the defined end date, you can change the time in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if maintenance window is enabled above. Use the date time picker to enter the start date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Ends	This field is only visible if maintenance window is enabled above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. ▪ Select object: Pause the current object if its parent object is in a Down status, or if it is paused by another dependency. Additionally, pause the current object if a specific other object in the device tree is in a Down status, or if it is paused by another dependency. Select below. <p> You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule.</p> <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the select object option is enabled above. Click on the reading-glass symbol and use the object selector ^[240] to choose an object on which the current object will be dependent on.
Dependency Delay (Sec.)	<p>This field is only visible if you select another object than the parent as dependency type. Define a time span in seconds for dependency delay.</p> <p>After the master object for this dependency comes back to an Up status, monitoring of the depending objects will be additionally delayed by the defined time span. This can help avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

ADVANCED NETWORK ANALYSIS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Unusual Detection Define if you want to benefit from [unusual detection](#)^[336] for sensors. You can configure the behavior of unusual detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate unusual detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. Sensors affected by this setting will turn to orange color ([unusual sensor status](#)^[195]) if PRTG detects unusual activity.
- **Disabled:** Do not activate unusual detection. PRTG will ignore unusual values for sensors affected by this setting. These sensors will not show an unusual sensor status.

Similar Sensors Detection Define if you want to activate [Similar Sensors](#)^[209] analysis. You can configure the depth of analysis of similar sensors detection (or disable it completely) in the [system settings](#)^[336]. Choose between:

- **Enabled:** Activate similar sensors detection for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree. PRTG considers all sensors affected by this setting during similarity analysis.

ADVANCED NETWORK ANALYSIS

- **Disabled:** Do not activate similar sensors detection. PRTG will not consider sensors affected by this setting during similarity analysis.
- System Information Define if you want to retrieve and show [System Information](#)^[222] for your devices. Choose between:
- **Enabled:** Activate the system information feature for this object and, by default, for all objects underneath in the [hierarchy](#)^[133] of the device tree.
 - **Disabled:** Do not activate system information.
-  **System Information** is enabled by default. To retrieve the data, PRTG will automatically use **Credentials for Windows Systems** and **Credentials for SNMP Devices** as defined in the [device settings](#)^[402] or as [inherited](#)^[133] from a parent object like the **Root** group. Please consider this when you monitor devices outside the local network, especially when using **SNMP v1** or **v2c** that do not provide encryption.
-  This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notifications

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs. In an object's detail page, click the **Notifications** tab to change sensor notification triggers. The defined triggers will be inherited down to sensor level. For detailed information, see [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see [Object Settings](#)^[217] section.

More

Knowledge Base: How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- <https://kb.paessler.com/en/topic/313>

Knowledge Base: How can I add my own device icons for use in the PRTG web interface?

- <https://kb.paessler.com/en/topic/7313>

Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?

- <https://kb.paessler.com/en/topic/7363>

Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?

- <https://kb.paessler.com/en/topic/43503>

7.8 Sensor Settings

There are more than 200 different sensor types available. In the **Add Sensor** dialog, all sensors are categorized into groups to help you quickly find what you need. Once you are familiar with the interface, you will probably enter the first letters of a sensor type's name into the **Search** field in the upper-left corner and get to a sensor even faster.

Available Sensor Types

There is a dedicated manual section for every sensor type with details about the available settings.

 For more information, see the [List of Available Sensors](#)^[429].

 For sensor settings, there is also multi-edit available. This enables you to change properties of many sensors at a time. For more details, see section [Multi-Edit Lists](#)^[3197].

To detect unexpected correlations between your network components, PRTG provides a [Similar Sensors](#)^[209] analysis.

Sensor Settings Overview

For information about sensor settings, see the following sections:

- [Sensor Settings—List of Available Sensor Types](#)^{[428][429]}
- [Additional Sensor Types \(Custom Sensors\)](#)^[3155]
- [Sensor Channels Settings](#)^[3160]
- [Sensor Notification Triggers Settings](#)^[3170]

7.8.1 List of Available Sensor Types

This chapter lists all available sensors, arranged both by different categories and in alphabetical order.

i In the [Add a Sensor](#)^[325] assistant, PRTG offers you various options to easily filter for fitting sensor types.

- [Common Sensors](#)^[429]
- [Bandwidth Monitoring Sensors](#)^[430]
- [Web Servers \(HTTP\) Sensors](#)^[430]
- [SNMP Sensors](#)^[431]
- [Windows WMI/Performance Counters Sensors](#)^[433]
- [Linux/Unix/OS X Sensors](#)^[434]
- [Virtual Servers Sensors](#)^[435]
- [Mail Servers Sensors](#)^[435]
- [Database Servers Sensors](#)^[436]
- [Storage and File Servers Sensors](#)^[436]
- [Various Servers Sensors](#)^[438]
- [VoIP and QoS Sensors](#)^[439]
- [Hardware Parameters Sensors](#)^[439]
- [Cloud Services Sensors](#)^[441]
- [Custom Sensors](#)^[441]
- [eHealth Sensors](#)^[442]
- [PRTG Internal Sensors](#)^[442]
- [All Sensors in Alphabetical Order](#)^[442]
- [Script World Sensors](#)^[450]
- [IoT Sensors](#)^[452]
- [More](#)^[452]

Common Sensors

- [Cloud HTTP Sensor](#)^[619]
- [Cloud Ping Sensor](#)^[629]
- [HTTP Sensor](#)^[955]
- [Ping Sensor](#)^[1529]
- [Port Sensor](#)^[1556]
- [Port Range Sensor](#)^[1566]

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP Traffic Sensor](#)  2467
- [SSL Certificate Sensor](#)  2635
- [SSL Security Check Sensor](#)  2646
- [Windows Network Card Sensor](#)  2793

Bandwidth Monitoring Sensors

- [IPFIX Sensor](#)  1186
- [IPFIX \(Custom\) Sensor](#)  1200
- [jFlow V5 Sensor](#)  1223
- [jFlow V5 \(Custom\) Sensor](#)  1237
- [NetFlow V5 Sensor](#)  1403
- [NetFlow V5 \(Custom\) Sensor](#)  1417
- [NetFlow V9 Sensor](#)  1430
- [NetFlow V9 \(Custom\) Sensor](#)  1444
- [Packet Sniffer Sensor](#)  1484
- [Packet Sniffer \(Custom\) Sensor](#)  1497
- [sFlow Sensor](#)  1740
- [sFlow \(Custom\) Sensor](#)  1754
- [SNMP Cisco ADSL Sensor](#)  1847
- [SNMP Cisco ASA VPN Traffic Sensor](#)  1866
- [SNMP Library Sensor](#)  2237
- [SNMP NetApp Network Interface Sensor](#)  2343
- [SNMP RMON Sensor](#)  2405
- [SNMP Traffic Sensor](#)  2467
- [Windows Network Card Sensor](#)  2793

Web Servers (HTTP) Sensors

- [Cloud HTTP Sensor](#)  619
- [Common SaaS Sensor](#)  644
- [HTTP Sensor](#)  955
- [HTTP Advanced Sensor](#)  965
- [HTTP Apache ModStatus PerfStats Sensor](#)  982
- [HTTP Apache ModStatus Totals Sensor](#)  992
- [HTTP Content Sensor](#)  1002
- [HTTP Data Advanced Sensor](#)  1014

- [HTTP Full Web Page Sensor](#)  1027
- [HTTP IoT Push Data Advanced Sensor](#)  1038
- [HTTP Push Count Sensor](#)  1049
- [HTTP Push Data Sensor](#)  1059
- [HTTP Push Data Advanced Sensor](#)  1070
- [HTTP Transaction Sensor](#)  1081
- [HTTP XML/REST Value Sensor](#)  1095
- [REST Custom Sensor](#)  1646
- [SSL Certificate Sensor](#)  2635
- [SSL Security Check Sensor](#)  2646
- [Windows IIS Application Sensor](#)  2772

SNMP Sensors

- [SNMP APC Hardware Sensor](#)  1829
- [SNMP Buffalo TS System Health Sensor](#)  1838
- [SNMP Cisco ADSL Sensor](#)  1847
- [SNMP Cisco ASA VPN Connections Sensor](#)  1856
- [SNMP Cisco ASA VPN Traffic Sensor](#)  1866
- [SNMP Cisco ASA VPN Users Sensor](#)  1877
- [SNMP Cisco CBooS Sensor](#)  1887
- [SNMP Cisco System Health Sensor](#)  1896
- [SNMP Cisco UCS Blade Sensor](#)  1905
- [SNMP Cisco UCS Chassis Sensor](#)  1914
- [SNMP Cisco UCS Sensor](#)  1923
- [SNMP Cisco UCS System Health Sensor](#)  1932
- [SNMP CPU Load Sensor](#)  1941
- [SNMP Custom Sensor](#)  1949
- [SNMP Custom Advanced Sensor](#)  1959
- [SNMP Custom String Sensor](#)  1970
- [SNMP Custom String Lookup Sensor](#)  1982
- [SNMP Custom Table Sensor](#)  1992
- [SNMP Dell EqualLogic Logical Disk Sensor](#)  2004
- [SNMP Dell EqualLogic Member Health Sensor](#)  2013
- [SNMP Dell EqualLogic Physical Disk Sensor](#)  2023

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP Dell Hardware Sensor](#)  2032
- [SNMP Dell PowerEdge Physical Disk Sensor](#)  2042
- [SNMP Dell PowerEdge System Health Sensor](#)  2052
- [SNMP Disk Free Sensor](#)  2063
- [SNMP Fujitsu System Health Sensor](#)  2072
- [SNMP Hardware Status Sensor](#)  2082
- [SNMP HP BladeSystem Server Blade Sensor](#)  2091
- [SNMP HP BladeSystem System Health Sensor](#)  2100
- [SNMP HP LaserJet Hardware Sensor](#)  2108
- [SNMP HP ProLiant Logical Disk Sensor](#)  2117
- [SNMP HP ProLiant Memory Controller Sensor](#)  2126
- [SNMP HP ProLiant Network Interface Sensor](#)  2136
- [SNMP HP ProLiant Physical Disk Sensor](#)  2146
- [SNMP HP ProLiant System Health Sensor](#)  2156
- [SNMP IBM System X Logical Disk Sensor](#)  2168
- [SNMP IBM System X Physical Disk Sensor](#)  2175
- [SNMP IBM System X Physical Memory Sensor](#)  2184
- [SNMP IBM System X System Health Sensor](#)  2193
- [SNMP interSeptor Pro Environment Sensor](#)  2203
- [SNMP Juniper System Health Sensor](#)  2212
- [SNMP LenovoEMC Physical Disk Sensor](#)  2220
- [SNMP LenovoEMC System Health Sensor](#)  2229
- [SNMP Library Sensor](#)  2237
- [SNMP Linux Disk Free Sensor](#)  2251
- [SNMP Linux Load Average Sensor](#)  2263
- [SNMP Linux Meminfo Sensor](#)  2271
- [SNMP Linux Physical Disk Sensor](#)  2279
- [SNMP Memory Sensor](#)  2288
- [SNMP NetApp Disk Free Sensor](#)  2297
- [SNMP NetApp Enclosure Sensor](#)  2306
- [SNMP NetApp I/O Sensor](#)  2316
- [SNMP NetApp License Sensor](#)  2325
- [SNMP NetApp Logical Unit Sensor](#)  2334
- [SNMP NetApp Network Interface Sensor](#)  2343

- [SNMP NetApp System Health Sensor](#)  2362
- [SNMP Poseidon Environment Sensor](#)  2361
- [SNMP Printer Sensor](#)  2370
- [SNMP QNAP Logical Disk Sensor](#)  2378
- [SNMP QNAP Physical Disk Sensor](#)  2387
- [SNMP QNAP System Health Sensor](#)  2396
- [SNMP RMON Sensor](#)  2405
- [SNMP SonicWall System Health Sensor](#)  2416
- [SNMP SonicWall VPN Traffic Sensor](#)  2424
- [SNMP Synology Logical Disk Sensor](#)  2433
- [SNMP Synology Physical Disk Sensor](#)  2442
- [SNMP Synology System Health Sensor](#)  2451
- [SNMP System Uptime Sensor](#)  2459
- [SNMP Traffic Sensor](#)  2467
- [SNMP Trap Receiver Sensor](#)  2479
- [SNMP Windows Service Sensor](#)  2492

Windows WMI/Performance Counters Sensors

- [Active Directory Replication Errors Sensor](#)  453
- [Event Log \(Windows API\) Sensor](#)  761
- [PerfCounter Custom Sensor](#)  1509
- [PerfCounter IIS Application Pool Sensor](#)  1519
- [Windows IIS 6.0 SMTP Received Sensor](#)  2754
- [Windows IIS 6.0 SMTP Sent Sensor](#)  2763
- [Windows IIS Application Pool Sensor](#)  1519
- [Windows CPU Load Sensor](#)  2744
- [Windows MSMQ Queue Length Sensor](#)  2762
- [Windows Network Card Sensor](#)  2793
- [Windows Pagefile Sensor](#)  2805
- [Windows Physical Disk I/O Sensor](#)  2815
- [Windows Print Queue Sensor](#)  2826
- [Windows Process Sensor](#)  2837
- [Windows System Uptime Sensor](#)  2848
- [Windows Updates Status \(PowerShell\) Sensor](#)  2857

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [WMI Custom Sensor](#)  2867
- [WMI Custom String Sensor](#)  2877
- [WMI Event Log Sensor](#)  2889
- [WMI Exchange Server Sensor](#)  2902
- [WMI Exchange Transport Queue Sensor](#)  2913
- [WMI File Sensor](#)  2924
- [WMI Free Disk Space \(Multi Disk\) Sensor](#)  2933
- [WMI HDD Health Sensor](#)  2945
- [WMI Logical Disk I/O Sensor](#)  2956
- [WMI Memory Sensor](#)  2966
- [WMI Microsoft SQL Server 2005 Sensor](#)  2975
- [WMI Microsoft SQL Server 2008 Sensor](#)  2988
- [WMI Microsoft SQL Server 2012 Sensor](#)  3000
- [WMI Microsoft SQL Server 2014 Sensor](#)  3012
- [WMI Microsoft SQL Server 2016 Sensor](#)  3024
- [WMI Microsoft SQL Server 2017 Sensor](#)  3036
- [WMI Remote Ping Sensor](#)  3046
- [WMI Security Center Sensor](#)  3057
- [WMI Service Sensor](#)  3067
- [WMI Share Sensor](#)  3077
- [WMI SharePoint Process Sensor](#)  3088
- [WMI Terminal Services \(Windows 2008+\) Sensor](#)  3097
- [WMI Terminal Services \(Windows XP/Vista/2003\) Sensor](#)  3106
- [WMI UTC Time Sensor](#)  3115
- [WMI Vital System Data \(V2\) Sensor](#)  3124
- [WMI Volume Sensor](#)  3134
- [WSUS Statistics Sensor](#)  3144

Linux/Unix/OS X Sensors

- [Python Script Advanced Sensor](#)  1597
- [SNMP Linux Disk Free Sensor](#)  2251
- [SNMP Linux Load Average Sensor](#)  2263
- [SNMP Linux Meminfo Sensor](#)  2271
- [SNMP Linux Physical Disk Sensor](#)  2279

- [SSH Disk Free Sensor](#)  2507
- [SSH INodes Free Sensor](#)  2522
- [SSH Load Average Sensor](#)  2532
- [SSH Meminfo Sensor](#)  2542
- [SSH Remote Ping Sensor](#)  2552
- [SSH Script Sensor](#)  2607
- [SSH Script Advanced Sensor](#)  2622
- [SSH SAN Enclosure Sensor](#)  2562
- [SSH SAN Logical Disk Sensor](#)  2573
- [SSH SAN Physical Disk Sensor](#)  2584
- [SSH SAN System Health Sensor](#)  2596

Virtual Servers Sensors

- [Citrix XenServer Host Sensor](#)  599
- [Citrix XenServer Virtual Machine Sensor](#)  609
- [Docker Container Status Sensor](#)  730
- [Hyper-V Cluster Shared Volume Disk Free Sensor](#)  1110
- [Hyper-V Host Server Sensor](#)  1121
- [Hyper-V Virtual Machine Sensor](#)  1130
- [Hyper-V Virtual Network Adapter Sensor](#)  1141
- [Hyper-V Virtual Storage Device Sensor](#)  1152
- [VMware Datastore \(SOAP\) Sensor](#)  2692
- [VMware Host Hardware \(WBEM\) Sensor](#)  2703
- [VMware Host Hardware Status \(SOAP\) Sensor](#)  2713
- [VMware Host Performance \(SOAP\) Sensor](#)  2723
- [VMware Virtual Machine \(SOAP\) Sensor](#)  2733

Mail Servers Sensors

- [Exchange Backup \(PowerShell\) Sensor](#)  773
- [Exchange Database \(PowerShell\) Sensor](#)  783
- [Exchange Database DAG \(PowerShell\) Sensor](#)  794
- [Exchange Mail Queue \(PowerShell\) Sensor](#)  804
- [Exchange Mailbox \(PowerShell\) Sensor](#)  814
- [Exchange Public Folder \(PowerShell\) Sensor](#)  824
- [IMAP Sensor](#)  1162

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [IP on DNS Blacklist Sensor](#)  1177
- [POP3 Sensor](#)  1547
- [SMTP Sensor](#)  1795
- [SMTP&IMAP Round Trip Sensor](#)  1805
- [SMTP&POP3 Round Trip Sensor](#)  1817
- [SSL Security Check Sensor](#)  2646
- [WMI Exchange Server Sensor](#)  2902
- [WMI Exchange Transport Queue Sensor](#)  2913
- [Windows IIS 6.0 SMTP Received Sensor](#)  2754
- [Windows IIS 6.0 SMTP Sent Sensor](#)  2763

Database Servers Sensors

- [ADO SQL v2 Sensor](#)  463
- [Microsoft SQL v2 Sensor](#)  1267
- [MySQL v2 Sensor](#)  1284
- [Oracle SQL v2 Sensor](#)  1457
- [Oracle Tablespace Sensor](#)  1474
- [PostgreSQL Sensor](#)  1574
- [WMI Microsoft SQL Server 2005 Sensor](#)  2975
- [WMI Microsoft SQL Server 2008 Sensor](#)  2989
- [WMI Microsoft SQL Server 2012 Sensor](#)  3000
- [WMI Microsoft SQL Server 2014 Sensor](#)  3012
- [WMI Microsoft SQL Server 2016 Sensor](#)  3024
- [WMI Microsoft SQL Server 2017 Sensor](#)  3036

Storage and File Servers Sensors

- [Dell PowerVault MDi Logical Disk Sensor](#)  659
- [Dell PowerVault MDi Physical Disk Sensor](#)  669
- [Enterprise Virtual Array Sensor](#)  751
- [File Sensor](#)  860
- [File Content Sensor](#)  870
- [Folder Sensor](#)  880
- [FTP Sensor](#)  891
- [FTP Server File Count Sensor](#)  900
- [Hyper-V Cluster Shared Volume Disk Free Sensor](#)  1110

- [Hyper-V Virtual Storage Device Sensor](#)  1152
- [NetApp Aggregate Sensor](#)  1300
- [NetApp I/O Sensor](#)  1311
- [NetApp LIF Sensor](#)  1323
- [NetApp LUN Sensor](#)  1334
- [NetApp NIC Sensor](#)  1345
- [NetApp Physical Disk Sensor](#)  1358
- [NetApp SnapMirror Sensor](#)  1367
- [NetApp System Health Sensor](#)  1379
- [NetApp Volume Sensor](#)  1391
- [REST Dell EMC Capacity Sensor](#)  1671
- [REST Dell EMC File System Sensor](#)  1680
- [REST Dell EMC LUN Sensor](#)  1690
- [REST Dell EMC Pool Sensor](#)  1700
- [REST Dell EMC System Health Sensor](#)  1711
- [SFTP Secure File Transfer Protocol Sensor](#)  1767
- [Share Disk Free Sensor](#)  1777
- [SNMP Buffalo TS System Health Sensor](#)  1838
- [SNMP Cisco UCS Physical Disk Sensor](#)  1923
- [SNMP Dell EqualLogic Logical Disk Sensor](#)  2004
- [SNMP Dell EqualLogic Member Health Sensor](#)  2013
- [SNMP Dell EqualLogic Physical Disk Sensor](#)  2023
- [SNMP Dell PowerEdge Physical Disk Sensor](#)  2042
- [SNMP HP ProLiant Logical Disk Sensor](#)  2117
- [SNMP HP ProLiant Physical Disk Sensor](#)  2146
- [SNMP IBM System X Logical Disk Sensor](#)  2166
- [SNMP IBM System X Physical Disk Sensor](#)  2175
- [SNMP Linux Disk Free Sensor](#)  2251
- [SNMP Linux Physical Disk Sensor](#)  2279
- [SNMP LenovoEMC Physical Disk Sensor](#)  2220
- [SNMP LenovoEMC System Health Sensor](#)  2229
- [SNMP NetApp Disk Free Sensor](#)  2297
- [SNMP NetApp Enclosure Sensor](#)  2306
- [SNMP NetApp I/O Sensor](#)  2316

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP NetApp License Sensor](#)  2325
- [SNMP NetApp Logical Unit Sensor](#)  2334
- [SNMP NetApp Network Interface Sensor](#)  2343
- [SNMP NetApp System Health Sensor](#)  2352
- [SNMP QNAP Logical Disk Sensor](#)  2378
- [SNMP QNAP Physical Disk Sensor](#)  2387
- [SNMP QNAP System Health Sensor](#)  2396
- [SNMP Synology Logical Disk Sensor](#)  2433
- [SNMP Synology Physical Disk Sensor](#)  2442
- [SNMP Synology System Health Sensor](#)  2451
- [SSH SAN Enclosure Sensor](#)  2562
- [SSH SAN Logical Disk Sensor](#)  2573
- [SSH SAN Physical Disk Sensor](#)  2584
- [SSH SAN System Health Sensor](#)  2596
- [TFTP Sensor](#)  2675
- [VMware Datastore \(SOAP\) Sensor](#)  2692
- [Windows Physical Disk I/O Sensor](#)  2815
- [WMI File Sensor](#)  2924
- [WMI Free Disk Space \(Multi Disk\) Sensor](#)  2933
- [WMI Logical Disk I/O Sensor](#)  2956
- [WMI Volume Sensor](#)  3134

Various Servers Sensors

- [DHCP Sensor](#)  680
- [DNS Sensor](#)  721
- [IPMI System Health Sensor](#)  1213
- [LDAP Sensor](#)  1250
- [Ping Sensor](#)  1529
- [Ping Jitter Sensor](#)  1538
- [Port Sensor](#)  1556
- [Port Range Sensor](#)  1566
- [RADIUS v2 Sensor](#)  1628
- [RDP \(Remote Desktop\) Sensor](#)  1638
- [SNMP Trap Receiver Sensor](#)  2479

- [SNTP Sensor](#)  2500
- [Syslog Receiver Sensor](#)  2650
- [SSL Security Check Sensor](#)  2646
- [Traceroute Hop Count Sensor](#)  2683

VoIP and QoS Sensors

- [Cisco IP SLA Sensor](#)  589
- [SIP Options Ping Sensor](#)  1786
- [QoS \(Quality of Service\) One Way Sensor](#)  1608
- [QoS \(Quality of Service\) Round Trip Sensor](#)  1617
- [SNMP Cisco CBQoS Sensor](#)  1867

Hardware Parameter Sensors

- [Dell PowerVault MDi Logical Disk Sensor](#)  659
- [Dell PowerVault MDi Physical Disk Sensor](#)  669
- [Enterprise Virtual Array Sensor](#)  751
- [NetApp Aggregate Sensor](#)  1300
- [NetApp I/O Sensor](#)  1311
- [NetApp LIF Sensor](#)  1323
- [NetApp LUN Sensor](#)  1334
- [NetApp NIC Sensor](#)  1345
- [NetApp Physical Disk Sensor](#)  1366
- [NetApp SnapMirror Sensor](#)  1367
- [NetApp System Health Sensor](#)  1379
- [NetApp Volume Sensor](#)  1391
- [SNMP APC Hardware Sensor](#)  1829
- [SNMP Buffalo TS System Health Sensor](#)  1838
- [SNMP Cisco System Health Sensor](#)  1896
- [SNMP Cisco UCS Blade Sensor](#)  1905
- [SNMP Cisco UCS Chassis Sensor](#)  1914
- [SNMP Cisco UCS Physical Disk Sensor](#)  1923
- [SNMP Cisco UCS System Health Sensor](#)  1932
- [SNMP CPU Load Sensor](#)  1941
- [SNMP Dell EqualLogic Logical Disk Sensor](#)  2004
- [SNMP Dell EqualLogic Member Health Sensor](#)  2013

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP Dell EqualLogic Physical Disk Sensor](#) 
- [SNMP Dell Hardware Sensor](#) 
- [SNMP Dell PowerEdge Physical Disk Sensor](#) 
- [SNMP Dell PowerEdge System Health Sensor](#) 
- [SNMP Disk Free Sensor](#) 
- [SNMP Hardware Status Sensor](#) 
- [SNMP HP BladeSystem Blade Sensor](#) 
- [SNMP HP BladeSystem Enclosure System Health Sensor](#) 
- [SNMP HP LaserJet Hardware Sensor](#) 
- [SNMP HP ProLiant Memory Controller Sensor](#) 
- [SNMP HP ProLiant Network Interface Sensor](#) 
- [SNMP HP ProLiant Physical Disk Sensor](#) 
- [SNMP HP ProLiant System Health Sensor](#) 
- [SNMP IBM System X Physical Disk Sensor](#) 
- [SNMP IBM System X Physical Memory Sensor](#) 
- [SNMP IBM System X System Health Sensor](#) 
- [SNMP Juniper NS System Health Sensor](#) 
- [SNMP LenovoEMC Physical Disk Sensor](#) 
- [SNMP LenovoEMC System Health Sensor](#) 
- [SNMP Library Sensor](#) 
- [SNMP Memory Sensor](#) 
- [SNMP NetApp I/O Sensor](#) 
- [SNMP NetApp Enclosure Sensor](#) 
- [SNMP NetApp Logical Unit Sensor](#) 
- [SNMP NetApp Network Interface Sensor](#) 
- [SNMP NetApp System Health Sensor](#) 
- [SNMP QNAP Physical Disk Sensor](#) 
- [SNMP QNAP System Health Sensor](#) 
- [SNMP SonicWall System Health Sensor](#) 
- [SNMP SonicWall VPN Traffic Sensor](#) 
- [SNMP Synology Physical Disk Sensor](#) 
- [SNMP Synology System Health Sensor](#) 
- [SSH SAN Enclosure Sensor](#) 
- [SSH SAN Logical Disk Sensor](#) 

- [SSH SAN Physical Disk Sensor](#)  2584
- [SSH SAN System Health Sensor](#)  2596
- [WMI HDD Health Sensor](#)  2945

Cloud Services Sensors

- [Amazon CloudWatch Alarm Sensor](#)  479
- [Amazon CloudWatch EBS Sensor](#)  489
- [Amazon CloudWatch EC2 Sensor](#)  501
- [Amazon CloudWatch ElastiCache Sensor](#)  514
- [Amazon CloudWatch ELB Sensor](#)  527
- [Amazon CloudWatch RDS Sensor](#)  539
- [Amazon CloudWatch SNS Sensor](#)  552
- [Amazon CloudWatch SQS Sensor](#)  564
- [Common SaaS Sensor](#)  644
- [Dropbox Sensor](#)  741
- [GitLab Build Status Sensor](#)  911
- [Google Analytics Sensor](#)  921
- [Google Drive Sensor](#)  934
- [Microsoft OneDrive Sensor](#)  1257

Custom Sensors

- [EXE/Script Sensor](#)  834
- [EXE/Script Advanced Sensor](#)  847
- [IPFIX \(Custom\) Sensor](#)  1200
- [jFlow V5 \(Custom\) Sensor](#)  1237
- [NetFlow V5 \(Custom\) Sensor](#)  1417
- [NetFlow V9 \(Custom\) Sensor](#)  1444
- [Packet Sniffer \(Custom\) Sensor](#)  1497
- [Python Script Advanced Sensor](#)  1597
- [REST Custom Sensor](#)  1646
- [Sensor Factory Sensor](#)  1720
- [sFlow \(Custom\) Sensor](#)  1754
- [SNMP Custom Sensor](#)  1949
- [SNMP Custom Advanced Sensor](#)  1959
- [SNMP Custom Lookup Sensor](#)  1982

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP Custom String Sensor](#)^[1970]
- [SNMP Custom Table Sensor](#)^[1992]
- [SSH Script Sensor](#)^[2607]
- [SSH Script Advanced Sensor](#)^[2622]
- [WMI Custom Sensor](#)^[2867]
- [WMI Custom String Sensor](#)^[2877]

eHealth Sensors

- [DICOM Bandwidth Sensor](#)^[691]
- [DICOM C-ECHO Sensor](#)^[701]
- [DICOM Query/Retrieve Sensor](#)^[710]
- [HL7 Sensor](#)^[944]

PRTG Internal Sensors

- [Cluster Health Sensor](#)^[638]
- [Core Health Sensor](#)^[652]
- [Probe Health Sensor](#)^[1590]
- [System Health Sensor](#)^[2669]

All Sensors in Alphabetical Order

The version numbers show when the respective sensor type was originally introduced to PRTG.

- [Active Directory Replication Errors Sensor](#)^[453] (v8.3.0)
- [ADO SQL v2 Sensor](#)^[463] (v16.x.24)
- [Amazon CloudWatch Alarm Sensor](#)^[479] (v16.x.22)
- [Amazon CloudWatch EBS Sensor](#)^[489] (v15.x.19)
- [Amazon CloudWatch EC2 Sensor](#)^[501] (v15.x.19)
- [Amazon CloudWatch ElastiCache Sensor](#)^[514] (v15.x.19)
- [Amazon CloudWatch ELB Sensor](#)^[527] (v15.x.19)
- [Amazon CloudWatch RDS Sensor](#)^[539] (v15.x.19)
- [Amazon CloudWatch SNS Sensor](#)^[552] (v15.x.19)
- [Amazon CloudWatch SQS Sensor](#)^[564] (v15.x.19)
- [Business Process Sensor](#)^[576] (v15.x.20)
- [Cisco IP SLA Sensor](#)^[589] (v7)
- [Citrix XenServer Host Sensor](#)^[599] (v12.x.1)

- [Citrix XenServer Virtual Machine Sensor](#)^[609] (v8.1.0)
- [Cloud HTTP Sensor](#)^[619] (v14.x.14)
- [Cloud Ping Sensor](#)^[629] (v14.x.14)
- [Cluster Health Sensor](#)^[638] (v9.1.0)
- [Common SaaS Sensor](#)^[644] (v15.x.19)
- [Core Health Sensor](#)^[652] (v9.1.0)
- [Dell PowerVault MDi Logical Disk Sensor](#)^[659] (v12.x.1)
- [Dell PowerVault MDi Physical Disk Sensor](#)^[669] (v14.x.13)
- [DHCP Sensor](#)^[680] (v8.2.0)
- [DICOM Bandwidth Sensor](#)^[691] (v18.1.38)
- [DICOM C-ECHO Sensor](#)^[701] (v18.1.38)
- [DICOM Query/Retrieve Sensor](#)^[710] (v18.1.38)
- [DNS Sensor](#)^[721] (v7)
- [Docker Container Status Sensor](#)^[730] (v16.x.22)
- [Dropbox Sensor](#)^[741] (v15.x.19)
- [Enterprise Virtual Array Sensor](#)^[751] (v13.x.6)
- [Event Log \(Windows API\) Sensor](#)^[761] (v7)
- [Exchange Backup \(PowerShell\) Sensor](#)^[773] (v13.x.5)
- [Exchange Database \(PowerShell\) Sensor](#)^[783] (v13.x.5)
- [Exchange Database DAG \(PowerShell\) Sensor](#)^[794] (v15.x.18)
- [Exchange Mail Queue \(PowerShell\) Sensor](#)^[804] (v13.x.5)
- [Exchange Mailbox \(PowerShell\) Sensor](#)^[814] (v13.x.5)
- [Exchange Public Folder \(PowerShell\) Sensor](#)^[824] (v13.x.5)
- [EXE/Script Sensor](#)^[834] (v7)
- [EXE/Script Advanced Sensor](#)^[847] (v7)
- [File Sensor](#)^[860] (v7)
- [File Content Sensor](#)^[870] (v7)
- [Folder Sensor](#)^[880] (v7)
- [FTP Sensor](#)^[891] (v7)
- [FTP Server File Count Sensor](#)^[900] (v8.3.0)
- [GitLab Build Status Sensor](#)^[911] (v16.3.26)
- [Google Analytics Sensor](#)^[921] (v15.x.19)
- [Google Drive Sensor](#)^[934] (v15.x.19)
- [HL7 Sensor](#)^[944] (v18.1.38)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [HTTP Sensor](#)^[955] (v7)
- [HTTP Advanced Sensor](#)^[965] (v7)
- [HTTP Apache ModStatus PerfStats Sensor](#)^[982] (v12.x.3)
- [HTTP Apache ModStatus Totals Sensor](#)^[992] (v12.x.3)
- [HTTP Content Sensor](#)^[1002] (v7)
- [HTTP Data Advanced Sensor](#)^[1014] (v15.x.16)
- [HTTP Full Web Page Sensor](#)^[1027] (v7)
- [HTTP IoT Push Data Advanced](#)^[1036] (v18.3.43)
- [HTTP Push Count Sensor](#)^[1049] (v13.4.8)
- [HTTP Push Data Sensor](#)^[1059] (v14.1.9)
- [HTTP Push Data Advanced Sensor](#)^[1070] (14.1.10)
- [HTTP Transaction Sensor](#)^[1081] (v7)
- [HTTP XML/REST Value Sensor](#)^[1095] (v8.3.0)
- [Hyper-V Cluster Shared Volume Disk Free Sensor](#)^[1110] (v12.3.4)
- [Hyper-V Host Server Sensor](#)^[1121] (v7)
- [Hyper-V Virtual Machine Sensor](#)^[1130] (v7)
- [Hyper-V Virtual Network Adapter Sensor](#)^[1141] (v9.1.0)
- [Hyper-V Virtual Storage Device Sensor](#)^[1152] (v12.4.4)
- [IMAP Sensor](#)^[1162] (v7)
- [IP on DNS Blacklist Sensor](#)^[1177] (v8.3.0)
- [IPFIX Sensor](#)^[1186] (v13.x.7)
- [IPFIX \(Custom\) Sensor](#)^[1200] (v13.x.7)
- [IPMI System Health Sensor](#)^[1213] (v14.x.11)
- [jFlow V5 Sensor](#)^[1223] (v8.2.0)
- [jFlow V5 \(Custom\) Sensor](#)^[1237] (v8.2.0)
- [LDAP Sensor](#)^[1250] (v8.1.0)
- [Microsoft OneDrive Sensor](#)^[1257] (v15.x.19)
- [Microsoft SQL v2 Sensor](#)^[1267] (v14.x.12)
- [MySQL v2 Sensor](#)^[1284] (v14.x.12)
- [NetApp Aggregate Sensor](#)^[1300] (v17.3.33)
- [NetApp I/O Sensor](#)^[1311] (v17.3.33)
- [NetApp LIF Sensor](#)^[1325] (v17.3.33)
- [NetApp LUN Sensor](#)^[1334] (v17.3.33)
- [NetApp NIC Sensor](#)^[1345] (v17.3.33)

- [NetApp Physical Disk Sensor](#)¹³⁸⁶ (v17.3.33)
- [NetApp SnapMirror Sensor](#)¹³⁶⁷ (v17.4.35)
- [NetApp System Health Sensor](#)¹³⁷⁹ (v17.3.33)
- [NetApp Volume Sensor](#)¹³⁹¹ (v17.3.33)
- [NetFlow V5 Sensor](#)¹⁴⁰³ (v7)
- [NetFlow V5 \(Custom\) Sensor](#)¹⁴¹⁷ (v7)
- [NetFlow V9 Sensor](#)¹⁴³⁰ (v7)
- [NetFlow V9 \(Custom\) Sensor](#)¹⁴⁴⁴ (v7)
- [Oracle SQL v2 Sensor](#)¹⁴⁵⁷ (v14.x.13)
- [Oracle Tablespace Sensor](#)¹⁴⁷⁴ (v15.x.18)
- [Packet Sniffer Sensor](#)¹⁴⁸⁴ (v7)
- [Packet Sniffer \(Custom\) Sensor](#)¹⁴⁹⁷ (v7)
- [PerfCounter Custom Sensor](#)¹⁵⁰⁹ (v12.x.3)
- [PerfCounter IIS Application Pool Sensor](#)¹⁵¹⁹ (v12.x.6)
- [Ping Sensor](#)¹⁵²⁹ (v7)
- [Ping Jitter Sensor](#)¹⁵³⁸ (v8.3.0)
- [POP3 Sensor](#)¹⁵⁴⁷ (v7)
- [Port Sensor](#)¹⁵⁵⁶ (v7)
- [Port Range Sensor](#)¹⁵⁶⁶ (v12.x.4)
- [PostgreSQL Sensor](#)¹⁵⁷⁴ (v14.x.12)
- [Probe Health Sensor](#)¹⁵⁹⁰ (v9.1.0)
- [Python Script Advanced Sensor](#)¹⁵⁹⁷ (v15.x.19)
- [QoS \(Quality of Service\) One Way Sensor](#)¹⁶⁰⁸ (v7)
- [QoS \(Quality of Service\) Round Trip Sensor](#)¹⁶¹⁷ (v9.1.0)
- [RADIUS v2 Sensor](#)¹⁶²⁶ (v14.x.13)
- [RDP \(Remote Desktop\) Sensor](#)¹⁶³⁸ (v7)
- [REST Custom Sensor](#)¹⁶⁴⁶ (v17.3.33)
- [REST Dell EMC Capacity Sensor](#)¹⁶⁷¹ (v17.4.37)
- [REST Dell EMC File System Sensor](#)¹⁶⁸⁰ (v17.4.37)
- [REST Dell EMC LUN Sensor](#)¹⁶⁹⁰ (v17.4.37)
- [REST Dell EMC Pool Sensor](#)¹⁷⁰⁰ (v17.4.37)
- [REST Dell EMC System Health Sensor](#)¹⁷¹¹ (v17.4.37)
- [Sensor Factory Sensor](#)¹⁷²⁰ (v7)
- [sFlow Sensor](#)¹⁷⁴⁰ (v7)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [sFlow \(Custom\) Sensor](#)^[1754] (v7)
- [SFTP Secure File Transfer Protocol Sensor](#)^[1767] (v12.x.6)
- [Share Disk Free Sensor](#)^[1777] (v7)
- [SIP Options Ping Sensor](#)^[1786] (v12.x.1)
- [SMTP Sensor](#)^[1796] (v7)
- [SMTP&IMAP Round Trip Sensor](#)^[1805] (v7)
- [SMTP&POP3 Round Trip Sensor](#)^[1817] (v7)
- [SNMP APC Hardware Sensor](#)^[1829] (v9.1.0)
- [SNMP Buffalo TS System Health Sensor](#)^[1836] (v17.1.29)
- [SNMP Cisco ADSL Sensor](#)^[1847] (v12.x.1)
- [SNMP Cisco ASA VPN Connections Sensor](#)^[1856] (v12.x.1)
- [SNMP Cisco ASA VPN Traffic Sensor](#)^[1866] (v12.x.1)
- [SNMP Cisco ASA VPN Users Sensor](#)^[1877] (v12.x.5)
- [SNMP Cisco CBQoS Sensor](#)^[1887] (v13.x.5)
- [SNMP Cisco System Health Sensor](#)^[1896] (v12.x.4)
- [SNMP Cisco UCS Blade Sensor](#)^[1905] (v14.x.14)
- [SNMP Cisco UCS Chassis Sensor](#)^[1914] (v13.x.8)
- [SNMP Cisco UCS Physical Disk Sensor](#)^[1923] (v14.1.10)
- [SNMP Cisco UCS System Health Sensor](#)^[1932] (v13.x.8)
- [SNMP CPU Load Sensor](#)^[1941] (v12.x.4)
- [SNMP Custom Sensor](#)^[1949] (v7)
- [SNMP Custom Advanced Sensor](#)^[1959] (v15.x.18)
- [SNMP Custom String Sensor](#)^[1970] (v9.1.0)
- [SNMP Custom String Lookup Sensor](#)^[1982] (v14.x.14)
- [SNMP Custom Table Sensor](#)^[1992] (v15x.18)
- [SNMP Dell EqualLogic Logical Disk Sensor](#)^[2004] (v16.x.24)
- [SNMP Dell EqualLogic Member Health Sensor](#)^[2013] (v16.x.24)
- [SNMP Dell EqualLogic Physical Disk Sensor](#)^[2023] (v16.x.24)
- [SNMP Dell Hardware Sensor](#)^[2032] (v7)
- [SNMP Dell PowerEdge Physical Disk Sensor](#)^[2042] (v12.x.4)
- [SNMP Dell PowerEdge System Health Sensor](#)^[2052] (v12.x.4)
- [SNMP Disk Free Sensor](#)^[2063] (v12.x.4)
- [SNMP Fujitsu System Health Sensor](#)^[2072] (v18.2.40)
- [SNMP Hardware Status Sensor](#)^[2082] (v13.x.5)

- [SNMP HP BladeSystem Blade Sensor](#)^[2091] (v15.x.18)
- [SNMP HP BladeSystem Enclosure System Health Sensor](#)^[2100] (v15.x.18)
- [SNMP HP LaserJet Hardware Sensor](#)^[2108] (v9.1.0)
- [SNMP HP ProLiant Logical Disk Sensor](#)^[2117] (v12.x.6)
- [SNMP HP ProLiant Memory Controller Sensor](#)^[2126] (v12.x.6)
- [SNMP HP ProLiant Network Interface Sensor](#)^[2136] (v12.x.4)
- [SNMP HP ProLiant Physical Disk Sensor](#)^[2146] (v12.x.6)
- [SNMP HP ProLiant System Health Sensor](#)^[2156] (v12.x.4)
- [SNMP IBM System X Logical Disk Sensor](#)^[2166] (v13.x.4)
- [SNMP IBM System X Physical Disk Sensor](#)^[2175] (v13.x.4)
- [SNMP IBM System X Physical Memory Sensor](#)^[2184] (v13.x.4)
- [SNMP IBM System X System Health Sensor](#)^[2193] (v13.x.4)
- [SNMP interSeptor Pro Environment Sensor](#)^[2203] (v14.1.10)
- [SNMP Juniper NS System Health Sensor](#)^[2212] (v15.2.16)
- [SNMP LenovoEMC Physical Disk Sensor](#)^[2220] (v13.x.8)
- [SNMP LenovoEMC System Health Sensor](#)^[2229] (v13.x.8)
- [SNMP Library Sensor](#)^[2237] (v7)
- [SNMP Linux Disk Free Sensor](#)^[2251] (v8.1.0)
- [SNMP Linux Load Average Sensor](#)^[2263] (v8.1.0)
- [SNMP Linux Meminfo Sensor](#)^[2271] (v8.1.0)
- [SNMP Linux Physical Disk Sensor](#)^[2279] (v13.x.5)
- [SNMP Memory Sensor](#)^[2288] (v12.x.4)
- [SNMP NetApp Disk Free Sensor](#)^[2297] (v12.x.3)
- [SNMP NetApp Enclosure Sensor](#)^[2306] (v12.x.4)
- [SNMP NetApp I/O Sensor](#)^[2316] (v12.x.3)
- [SNMP NetApp License Sensor](#)^[2325] (v12.x.4)
- [SNMP NetApp Logical Unit Sensor](#)^[2334] (v13.x.7)
- [SNMP NetApp Network Interface Sensor](#)^[2343] (v12.x.3)
- [SNMP NetApp System Health Sensor](#)^[2352] (v12.x.3)
- [SNMP Poseidon Environment Sensor](#)^[2361] (v13.x.5)
- [SNMP Printer Sensor](#)^[2370] (v14.x.11)
- [SNMP QNAP Logical Disk Sensor](#)^[2378] (v13.x.4)
- [SNMP QNAP Physical Disk Sensor](#)^[2387] (v13.x.4)
- [SNMP QNAP System Health Sensor](#)^[2396] (v13.x.4)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

1 List of Available Sensor Types

- [SNMP RMON Sensor](#)^[2405] (v12.x.1)
- [SNMP SonicWall System Health Sensor](#)^[2416] (v13.x.5)
- [SNMP SonicWall VPN Traffic Sensor](#)^[2424] (v13.x.6)
- [SNMP Synology Logical Disk Sensor](#)^[2433] (v13.x.4)
- [SNMP Synology Physical Disk Sensor](#)^[2442] (v13.x.4)
- [SNMP Synology System Health Sensor](#)^[2451] (v13.x.4)
- [SNMP System Uptime Sensor](#)^[2459] (v7)
- [SNMP Traffic Sensor](#)^[2467] (v7)
- [SNMP Trap Receiver Sensor](#)^[2479] (v7)
- [SNMP Windows Service Sensor](#)^[2492] (v13.x.8)
- [SNTP Sensor](#)^[2500] (v8.1.0)
- [SSH Disk Free Sensor](#)^[2507] (v8.1.0)
- [SSH INodes Free Sensor](#)^[2522] (v8.1.1)
- [SSH Load Average Sensor](#)^[2532] (v8.1.0)
- [SSH Meminfo Sensor](#)^[2542] (v8.1.0)
- [SSH Remote Ping Sensor](#)^[2562] (v12.x.1)
- [SSH SAN Enclosure Sensor](#)^[2562] (v14.x.12)
- [SSH SAN Logical Disk Sensor](#)^[2573] (v14.1.9)
- [SSH SAN Physical Disk Sensor](#)^[2584] (v14.1.9)
- [SSH SAN System Health Sensor](#)^[2596] (v14.1.9)
- [SSH Script Sensor](#)^[2607] (v12.x.1)
- [SSH Script Advanced Sensor](#)^[2622] (v12.x.6)
- [SSL Certificate Sensor](#)^[2635] (v15.x.19)
- [SSL Security Check Sensor](#)^[2646] (v14.x.12)
- [Syslog Receiver Sensor](#)^[2656] (v7)
- [System Health Sensor](#)^[2669] (v9.1.0)
- [TFTP Sensor](#)^[2675] (v8.1.0)
- [Traceroute Hop Count Sensor](#)^[2683] (v8.3.0)
- [VMware Datastore \(SOAP\) Sensor](#)^[2692] (v15.x.19)
- [VMware Host Hardware \(WBEM\) Sensor](#)^[2703] (v8.1.0)
- [VMware Host Hardware Status \(SOAP\) Sensor](#)^[2713] (v12.x.1)
- [VMware Host Performance \(SOAP\) Sensor](#)^[2723] (v12.x.1)
- [VMware Virtual Machine \(SOAP\) Sensor](#)^[2733] (v7)
- [Windows CPU Load Sensor](#)^[2744] (v7)

- [Windows IIS 6.0 SMTP Received Sensor](#)^[2754] (v8.1.0)
- [Windows IIS 6.0 SMTP Sent Sensor](#)^[2763] (v8.1.0)
- [Windows IIS Application Sensor](#)^[2772] (v12.x.1)
- [Windows MSMQ Queue Length Sensor](#)^[2782] (v8.3.0)
- [Windows Network Card Sensor](#)^[2793] (v7)
- [Windows Pagefile Sensor](#)^[2805] (v12.x.4)
- [Windows Physical Disk I/O Sensor](#)^[2815] (v16.x.24)
- [Windows Print Queue Sensor](#)^[2826] (v8.3.0)
- [Windows Process Sensor](#)^[2837] (v7)
- [Windows System Uptime Sensor](#)^[2848] (v8.1.0)
- [Windows Updates Status \(PowerShell\) Sensor](#)^[2857] (v13.x.6)
- [WMI Custom Sensor](#)^[2867] (v7)
- [WMI Custom String Sensor](#)^[2877] (v12.x.4)
- [WMI Event Log Sensor](#)^[2889] (v7)
- [WMI Exchange Server Sensor](#)^[2902] (v9)
- [WMI Exchange Transport Queue Sensor](#)^[2913] (v12.x.1)
- [WMI File Sensor](#)^[2924] (v7)
- [WMI Free Disk Space \(Multi Disk\) Sensor](#)^[2933] (v7)
- [WMI HDD Health Sensor](#)^[2945] (v12.x.1)
- [WMI Logical Disk I/O Sensor](#)^[2956] (v16.x.24)
- [WMI Memory Sensor](#)^[2966] (v7)
- [WMI Microsoft SQL Server 2005 Sensor](#)^[2975] (v8.1.0)
- [WMI Microsoft SQL Server 2008 Sensor](#)^[2988] (v8.1.0)
- [WMI Microsoft SQL Server 2012 Sensor](#)^[3000] (v12.x.6)
- [WMI Microsoft SQL Server 2014 Sensor](#)^[3012] (v14.x.13)
- [WMI Microsoft SQL Server 2016 Sensor](#)^[3024] (v16.x.26)
- [WMI Microsoft SQL Server 2017 Sensor](#)^[3036] (v18.x.42)
- [WMI Remote Ping Sensor](#)^[3048] (v12.x.1)
- [WMI Security Center Sensor](#)^[3057] (v9)
- [WMI Service Sensor](#)^[3067] (v7)
- [WMI Share Sensor](#)^[3077] (v8.1.0)
- [WMI SharePoint Process Sensor](#)^[3088] (v12.x.1)
- [WMI Terminal Services \(Windows 2008+\) Sensor](#)^[3097] (v8.1.0)
- [WMI Terminal Services \(Windows XP/Vista/2003\) Sensor](#)^[3106] (v8.1.0)

- [WMI UTC Time Sensor](#)³¹¹⁵ (v9.2.0)
- [WMI Vital System Data \(V2\) Sensor](#)³¹²⁴ (v7)
- [WMI Volume Sensor](#)³¹³⁴ (v7)
- [WSUS Statistics Sensor](#)³¹⁴⁴ (v9.1.0)

Script World Sensors

In addition to the built-in sensors, you can create your own sensors. Just write a script or a program and use it with a [custom sensor](#)⁴⁵². There are already many free, useful scripts, plugins, and add-ons for PRTG in the [PRTG Script World](#). You can directly open the Script World from the [Add Sensor](#)³²⁵ dialog in the PRTG web interface.

- Active Fileshare Sessions
- Active Lync Users, Inbound/Outbound Calls
- Active Windows Users
- AD Group Membership
- Advanced Exchange Server Metrics
- Age of McAfee Anti-Virus Signatures
- AllNet UPS
- Altaro Hyper-V Backup Monitoring
- Amazon AWS Costs
- APC Battery Replacement
- Aruba Wireless Controller Device Template
- Atlantis ILIO
- Automatic Services
- AWS Costs Sensor
- BGP Peer Status
- Brocade Switch Device Template
- BulkSMS Remaining Credits Sensor
- Ceph Cluster Storage Python Sensor
- Certain HTTP Response Code
- Citrix Environments
- Citrix NetScaler
- Configured Remote Probes
- DICOM and HL7
- Dynamic Windows Processes
- Exim Queue Length

- Find Groups and Devices with Auto-Discovery Enabled
- Google Search Appliance
- Historic Windows Events
- HP 3Par Enterprise Storage
- HP ProCurve Switch Version and Model
- HTTP Return Codes
- Hyper-V Replication
- iDirect Modem Sensor
- IP Addresses of Hops
- Kemp Load Balancer
- Linux Distributions that are Incompatible with the SSH Disk Free Sensor
- Linux Services
- Locked AD Users
- Microsoft Active Cluster Nodes
- Microsoft Teams
- Mounted Windows Volumes
- MySQL Replication
- MySQL Table Fragmentation
- NetApp Snapshot Age
- Nimble Storage Device Template
- PHP-FPM Status Page
- Processed MailScanner Mails
- PRTG Pester
- PRTG Uptime SLA Sensors
- Pure Storage FlashArray
- Quota Exceeding Exchange Mailboxes
- RabbitMQ Queues & Exchanges
- Resume All Paused Sensors
- SAP and SAP Database Monitoring
- SCVMM - Hyper-V and Virtual Machines
- Seatel Antenna Sensor
- Sensor Uptime Extractor
- Shadow Copy Age
- Slack

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
1 List of Available Sensor Types

- SNMP Debug Log Checking
- Subscriptions Monitoring with PRTG
- TXT DNS Records Monitoring
- Usernames Configured in PRTG
- Users Logged in to PRTG
- Veeam Backup and Replication
- VMware Horizon 7
- WatchGuard Firewall (Cluster or Non-Cluster) – Status Multi-WAN
- Website Login
- Windows DHCP Scope Status
- Windows Registry Value
- Workaround for Scripts Running Longer than 900 Seconds
- YUM Update Check

 Go to <https://www.paessler.com/script-world> and follow the instructions there to use these sensors.

IoT Sensors

- [HTTP IoT Push Data Advanced Sensor](#) 

More

PRTG Manual:

- [Additional Sensor Types \(Custom Sensors\)](#) 

Knowledge Base: Why do I encounter gaps in the graphs/data of my EXE sensors?

- <https://kb.paessler.com/en/topic/75735>

7.8.2 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor checks a Windows Domain Controller (DC) for replication errors.

It can show the following:

- Number of consecutive sync failures
- If the source is deleted
- If the scheduled sync is disabled
- Time of the last sync attempt
- Result of the last sync
- Time of the last sync success
- Number of modified consecutive sync failures
- Number of pending replication operations

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor Active Directory Replication Errors ☆☆☆☆

Ok

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Last Sync Result

0 #

Consecutive Sync Failu

0 #

Is Deleted Source

No

Last Sync Attempt

-53 s

Last Sync Success

-53 s

Modified Consecutive

0 #

Pending Replication O

0 #

Scheduled Sync Disabl

No

Channel	ID	Last Value	Minimum	Maximum	
Consecutive Sync Failures	5	0 #	0 #	0 #	
Downtime	-4				
Is Deleted Source	4	No	No	No	
Last Sync Attempt	8	-53 s	0 s	-43 s	
Last Sync Result	2	0 #	0 #	0 #	
Last Sync Success	9	-53 s	0 s	-43 s	
Modified Consecutive Sy...	6	0 #	0 #	0 #	
Pending Replication Ope...	7	0 #	0 #	0 #	
Scheduled Sync Disabled	3	No	No	No	

Active Directory Replication Errors Sensor

Sensor in Other Languages

Dutch: **Active Directory Replicatie Fouten**, French: **Erreurs de répliation Active Directory**, German: **Active Directory Replikationsfehler**, Japanese: **AD ? ? ? ? ? ? ? ? ? ? ? ?**, Portuguese: **Erros de replicação do Active Directory**, Russian: **Ошибки репликации Active Directory**, Simplified Chinese: **? ? ? ? ? ? ? ?**, Spanish: **Errores de replicación de Active Directory**

Remarks

- The device you add the sensor to must be a Domain Controller (DC).
 - [Requires](#)^[455] valid Windows domain credentials in the [settings of the parent device](#)^[407].
 - [Requires](#)^[455] the probe system to be part of the domain whose Active Directory you monitor.
 - [Requires](#)^[454] .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
 - We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
 - This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Member of Windows Domain

This sensor only works if the computer running the PRTG probe is part of the domain whose Active Directory you want to monitor. The probe runs either on the local system (on every node, if on a cluster probe), or on another system as [remote probe](#)^[3709]. If this requirement is not met, the sensor will not work. You have to add the sensor to a device that represents your Domain Controller (DC) in PRTG.

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the replications you want to monitor. PRTG creates one sensor for each replication neighbor you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Replication Neighbor	Select the replication neighbor whose replication you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
----------------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Replication Neighbor	Shows the replication neighbor whose replication this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
----------------------	---

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[335] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.3 ADO SQL v2 Sensor

The ADO SQL v2 sensor monitors a database using an ActiveX Data Objects (ADO) connection and executes a Structured Query Language (SQL) query. It can monitor any data source that is available via OLE DB (Object Linking and Embedding, Database) or ODBC (Open Database Connectivity).

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of the given query
- Number of rows that were addressed by the query (including **select** statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Remarks

- [Requires](#) ¹²⁶⁸ .NET 4.5 or later on the probe system.
- Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#) ⁴¹³ of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.

- PRTG Manual: [Monitoring Databases](#)^[3534] (includes an [example](#)^[3535] for channel value selection)
 - Knowledge Base: [How to setup the SQL v2 sensors in PRTG? Is there a guide?](#)
 - Knowledge Base: [How can I monitor strings from an SQL database and show a sensor status depending on it?](#)
 - Knowledge Base: [How can I monitor error tables in SQL databases?](#)
 - Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
 - Save the SQL script with the query into the `\Custom Sensors\sql\adosql` subfolder of your PRTG installation. See manual section [Data Storage](#)^[3731] for more information about how to find this path.
 - If you use an ODBC connection, you have to define the ODBC connection in the **Windows ODBC Connection Manager** first. If it is a 64-bit Windows, you need to define the ODBC connection as an ODBC 32-bit connection.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Connection String	<p>Enter the string that the sensor will use to connect to the database. For example, a connection string can look like this:</p> <pre>Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind</pre> <p>i For ODBC connections, you need to enter MSDASQL as provider, for example <code>Provider=MSDASQL;DSN=_my_odbc_sqlserver.</code></p> <p>i You can use the placeholders %dbloginuser and %dbloginpassword here. PRTG will replace them with the Credentials for Database Management Systems^[413] of the parent device.</p>
-------------------	--

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific `\Custom Sensors\sql` subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

 For more information on how to find this path, see section [Data Storage](#). By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: **SELECT AVG (UnitPrice) FROM Products**. If you want to use transactions, separate the individual steps with semicolons ";".

 Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

 See also this Knowledge Base article: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

SQL Variables

You can use the following variables in your query file to have them replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: **@prt g**
- Oracle SQL: **:prt g**
- ADO SQL: **?** (question mark)

@prt g, **:prt g**, and **?** behave like common SQL variables, so consider the general rules for SQL variables. For example, you cannot use a variable for a table in the FROM statement of a query.

Example for variables usage: **SELECT * FROM Table WHERE @prt g**

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the variables **@prt g** (Microsoft SQL, MySQL, PostgreSQL), or **:prt g** (Oracle SQL), or **?** (ADO SQL) in the SQL query, considering the general rules for SQL variables. Choose between:

DATA

- **Don't use input parameter (default):** Execute the SQL query file without using variables.
- **Use input parameter:** Execute an SQL query file that contains a variable. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter will replace the variable `@prtg` or `:prtg` or `?` in the SQL query, considering the general rules for SQL variables.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, `%sensorid` or `%deviceid`. For details, see section [Custom Sensors](#).

 Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default):** No transactions will be executed.
- **Use transaction and always rollback:** Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success:** Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Just execute the query:** If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows:** Choose this option if you perform a **SELECT** statement and want to monitor how many rows of the data table this statement returns.

DATA

- **Process data table:** Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with **SELECT** statements as well.

Handle DBNull in Channel Values as

This setting is only visible if you select **Process data table** above. Define the sensor behavior if **DBNull** is returned by the query. Choose between:

- **Error:** The sensor will show a **Down** status if **DBNull** is reported.
- **Number 0:** The sensor will recognize the result **DBNull** as a valid value and interpret it as the number **0**.

Select Channel Value by

This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between:

- **Column number:** The channel value will be determined by using the value in row 0 of the column whose number you specify below.
- **Column name:** The channel value will be determined by using the value in row 0 of the column whose name you specify below.
- **Row number:** The channel value will be determined by using the value in column 0 of the row whose number you specify below.
- **Key value pair:** The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found.

The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below.

 See manual section [Monitoring Databases](#)  for an [example](#)  for channel value selection.

Sensor Channel #x

This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for **Channel #1** without enabling it manually. For all other possible channels, choose between:

- **Disable:** This channel will not be added to the sensor.
- **Enable:** This channel will be added to the sensor. Define the settings as described above.

DATA

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Column Number This setting is only visible if you select **Column number** above. Provide the number of the column that will be used to determine the channel value in row 0. Please enter an integer value.

Sensor Channel #x Column Name This setting is only visible if you select **Column number** above. Provide the name of the column that will be used to determine the channel value in row 0. Please enter a string.

Sensor Channel #x Row Number This setting is only visible if you select **Row number** above. Provide the number of the row that will be used to determine the channel value in column 0. Please enter an integer value.

Sensor Channel #x Key This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.

Sensor Channel #x Mode This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended):** Shows the value as the sensor retrieves it from the data table.
- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from the data table. This mode is not compatible with the unit **Value Lookup**.

Sensor Channel #x Unit This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth

DATA

- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#).

 To use [lookups](#) with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x
Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a [lookup](#) file that you want to use with this channel.

Use Data Table Value in
Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable:** Do not use a custom sensor message.
- **Enable:** Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

DATA

Sensor Message Column Number	<p>This setting is only visible if you select Column number and Use Data Table Value in Sensor Message above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Column Name	<p>This setting is only visible if you select Column name and Use Data Table Value in Sensor Message above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Row Number	<p>This setting is only visible if you select Row number and Use Data Table Value in Sensor Message above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Key	<p>This setting is only visible if you select Key value pair and Use Data Table Value in Sensor Message above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message	<p>This setting is only visible if you select Use Data Table Value in Sensor Message above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.</p> <p>Example: The message is {0}</p>
If Sensor Message Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>(3170)</small> whenever the sensor value changes.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p>

DATA

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- <https://kb.paessler.com/en/topic/18183>

Knowledge Base: How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

PRTG Manual:

- [Monitoring Databases](#)³⁵³⁴

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.4 Amazon CloudWatch Alarm Sensor

The Amazon CloudWatch Alarm sensor monitors the status of an Amazon CloudWatch alarm. It reads the data via the AWS CloudWatch Application Programming Interface (API).

- This sensor can show the status of a configured alarm for a CloudWatch service.

✓ **Sensor Amazon CloudWatch Alarm** ★★★★☆
Threshold Crossed: 1 datapoint (54.92) was not greater than the threshold (1000.0).

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Alarm State

Ok

Channel	ID	Last Value	Minimum	Maximum	
Alarm State	1	Ok	Ok	Ok	⚙️
Downtime	-4				⚙️

Amazon CloudWatch Alarm Sensor

Sensor in Other Languages

Dutch: **Amazon CloudWatch Alarm**, French: **Alarme Amazon CloudWatch**, German: **Amazon CloudWatch Alarm**, Japanese: **Amazon CloudWatch** ? ? ? ? , Portuguese: **Amazon CloudWatch Alarmes**, Russian: **Сигнал тревоги Amazon CloudWatch**, Simplified Chinese: **Amazon CloudWatch** ? ? , Spanish: **Alarma Amazon CloudWatch**

Remarks

- The data you see in the sensor message is not necessarily the current data. It merely shows the reason for the current [status](#)^[195] and why the sensor changed to it. This means for the **Up** status, for example, that this data is as old as the amount of time that has passed since the last alarm disappeared.
- [Requires](#)^[480] access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- [Requires](#)^[480] .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- Names of configured alarms that you want to monitor must not contain double spaces.

- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#). If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for configured alarms on CloudWatch. This can take up to several minutes.

Select which alarm(s) you want to monitor. PRTG creates one sensor for each alarm you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the alarms you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).
----------	---

AMAZON CLOUDWATCH SPECIFIC

Region	<p>Shows the region in which the monitored AWS instance runs. It is one of the following regions:</p> <ul style="list-style-type: none"> ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (London) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore) ▪ Asia Pacific (Tokyo) ▪ Asia Pacific (Sydney) ▪ Asia Pacific (Seoul) ▪ Asia Pacific (Mumbai) ▪ South America (Sao Paulo) <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

AMAZON CLOUDWATCH SPECIFIC

- Result Handling** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

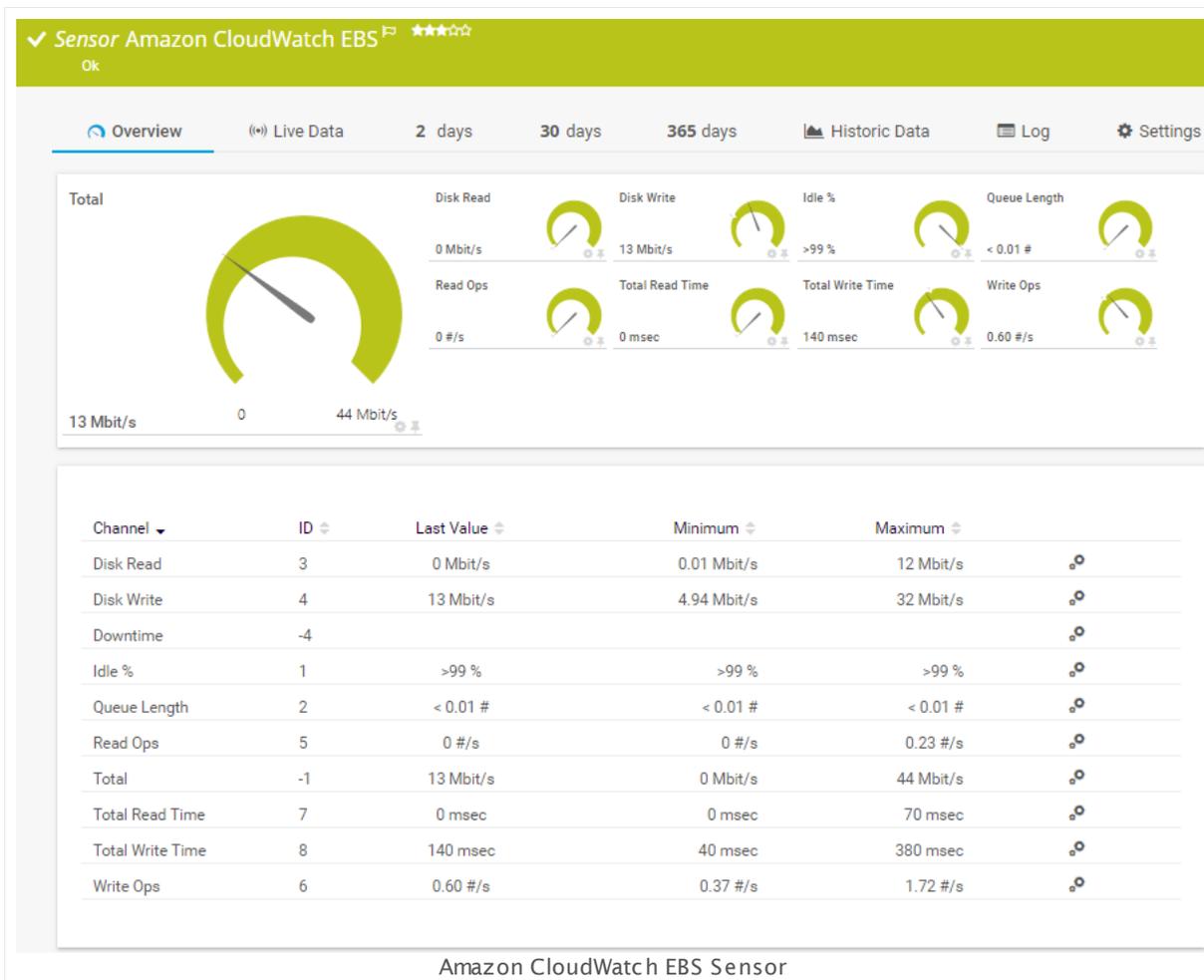
7.8.5 Amazon CloudWatch EBS Sensor

The Amazon CloudWatch EBS sensor monitors the performance of the Amazon Cloud service Elastic Block Store (EBS).

The sensor can show the following:

- Total volume of I/O operations
- Total disk read and write time
- Disk read and write speed
- Number of disk read and write operations per second
- Idle time with no submitted operations
- Number of read and write operations waiting to be completed

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#) in settings that are higher in the [Object Hierarchy](#), for example, in the [parent device settings](#).
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#) with a latency of **0 seconds** to receive all notifications for this sensor (**[...] for at least 0 seconds**).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#). If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services

Select the **Volume** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	<p>Shows the region in which the monitored AWS instance runs. It is one of the following regions:</p> <ul style="list-style-type: none"> ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (London) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore)
--------	---

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend
-----------------	--

SENSOR DISPLAY

on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- Elastic Block Store (EBS)
- VolumeTotalReadTime (Sum)
 - VolumeTotalWriteTime (Sum)
 - VolumeReadBytes (Sum)
 - VolumeWriteOps (Sum)
 - VolumeReadOps (Sum)
 - VolumeWriteBytes (Sum)
 - VolumeConsumedReadWriteOps (Sum)
 - VolumeQueueLength (Average)
 - VolumeIdleTime (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

Elastic Block Store (EBS) ▪ Volume

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.6 Amazon CloudWatch EC2 Sensor

The Amazon CloudWatch EC2 sensor monitors the performance of the Amazon Cloud service Elastic Cloud Computing (EC2).

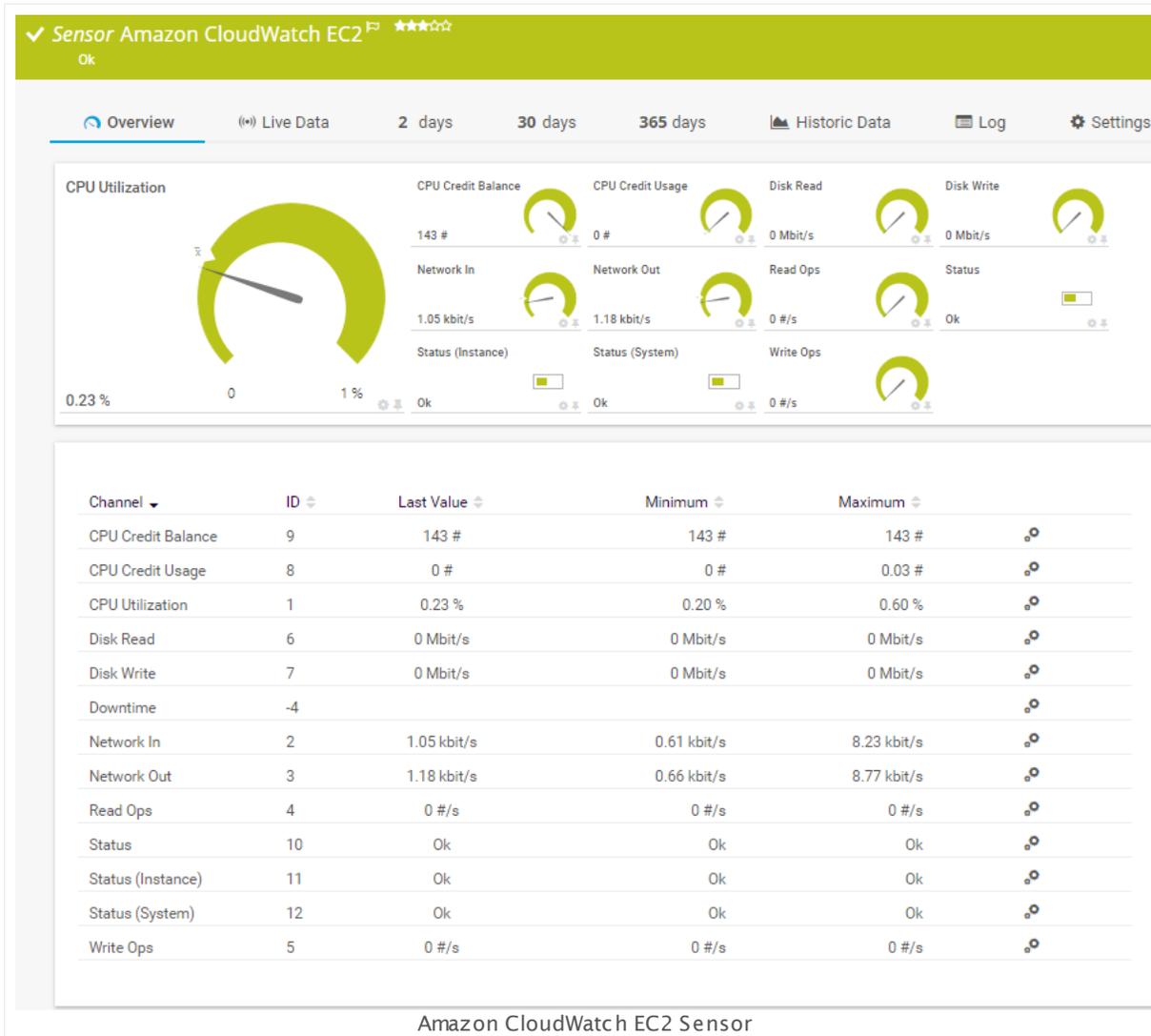
The sensor can show the following:

- CPU utilization
- Network load in and out
- Disk I/O:
 - Read and write speed
 - Number of disk read and write operations per second
- CPU credit usage and balance
- EC2 status checks

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

6 Amazon CloudWatch EC2 Sensor



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#)^[3170] with a latency of **0 seconds** to receive all notifications for this sensor ([\[...\] for at least 0 seconds](#)).

- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵¹ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the **Instances** or **Auto Scaling Groups** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3270], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region Shows the region in which the monitored AWS instance runs. It is one of the following regions:

- US East (Northern Virginia)
- US West (Oregon)
- US West (Northern California)
- Canada (Central)
- EU (Ireland)
- EU (London)
- EU (Frankfurt)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

AMAZON CLOUDWATCH SPECIFIC

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴.  This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.

Detailed Monitoring	<p>Choose whether you would like to import more or less detailed monitoring data from the AWS API. Choose between</p> <ul style="list-style-type: none"> ▪ Enabled: You get 1 dataset per minute. ▪ Disabled (default): You get 1 dataset per 5 minutes. <p> To use detailed monitoring in PRTG, you must also activate it for your monitored instance in the AWS web console.</p>
---------------------	---

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- | | |
|-----------------------------|--|
| Elastic Compute Cloud (EC2) | <ul style="list-style-type: none"> ▪ CPUUtilization (Average) ▪ NetworkIn (Sum) ▪ NetworkOut (Sum) ▪ DiskReadBytes (Sum) ▪ DiskReadOps (Sum) ▪ DiskWriteBytes (Sum) ▪ DiskWriteOps (Sum) ▪ CPUCreditUsage (Average) ▪ CPUCreditBalance (Average) ▪ StatusCheckFailed (Maximum) ▪ StatusCheckFailed_Instance (Maximum) ▪ StatusCheckFailed_System (Maximum) |
|-----------------------------|--|

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- Elastic Compute Cloud (EC2)
- Instance
 - Auto Scaling Group

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.7 Amazon CloudWatch ElastiCache Sensor

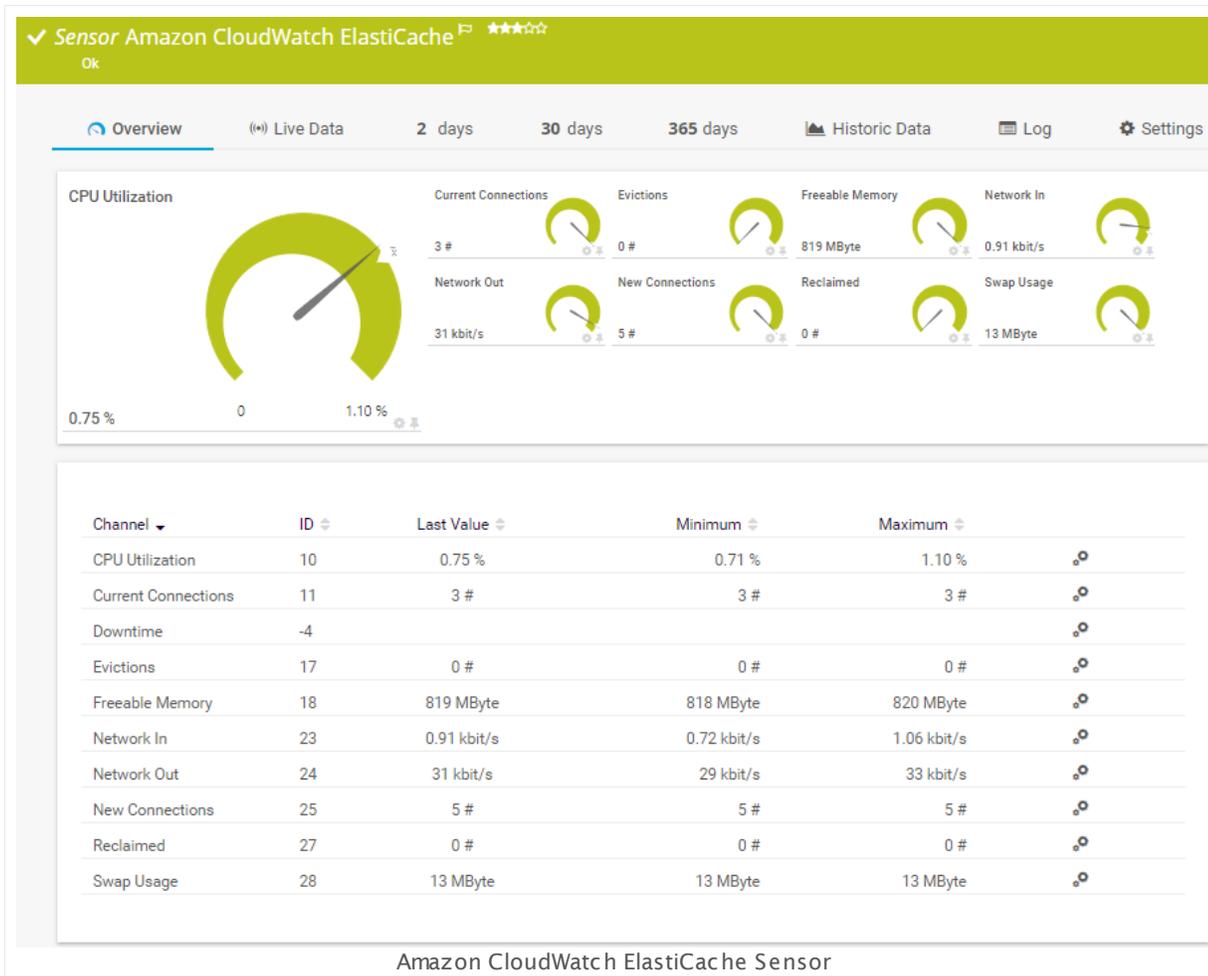
The Amazon CloudWatch ElastiCache sensor monitors the performance of the Amazon Cloud service ElastiCache.

The sensor can show the following:

- CPU utilization
- Memory
- Cache I/O
- Network I/O
- Cache Statistics

See [Supported Metrics](#) ⁵²⁴ for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#)^[3170] with a latency of **0 seconds** to receive all notifications for this sensor (**[...] for at least 0 seconds**).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services

Select the **Cache Clusters** or **Cache Cluster Nodes** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	<p>Shows the region in which the monitored AWS instance runs. It is one of the following regions:</p> <ul style="list-style-type: none"> ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (London) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore)
--------	---

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

ID

Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend

SENSOR DISPLAY

on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

 This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- | | |
|--------------------|--|
| ElastiCache | <ul style="list-style-type: none"> ▪ CPUUtilization (Average) ▪ CurrConnections (Average) ▪ CurrItems (Average) ▪ NewItems (Sum) ▪ NewConnections (Sum) ▪ FreeableMemory (Average) ▪ UnusedMemory (Average) ▪ SwapUsage (Average) ▪ BytesUsedForCacheItems (Average) ▪ BytesReadIntoMemcached (Sum) ▪ BytesWrittenOutFromMemcached (Sum) ▪ NetworkBytesIn (Sum) ▪ NetworkBytesOut (Sum) ▪ Evictions (Sum) ▪ Reclaimed (Sum) |
|--------------------|--|

AMAZON CLOUDWATCH METRICS

- CasBadval (Sum)
- CasHits (Sum)
- CasMisses (Sum)
- CmdFlush (Sum)
- Cmdget (Sum)
- Cmdset (Sum)
- DecrMisses (Sum)
- DecrHits (Sum)
- DeleteHits (Sum)
- DeleteMisses (Sum)
- GetHits (Sum)
- GetMisses (Sum)
- IncrHits (Sum)
- IncrMisses (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- | | |
|-------------|--|
| ElastiCache | <ul style="list-style-type: none">▪ Cache Cluster▪ Cache Cluster Node |
|-------------|--|

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.8 Amazon CloudWatch ELB Sensor

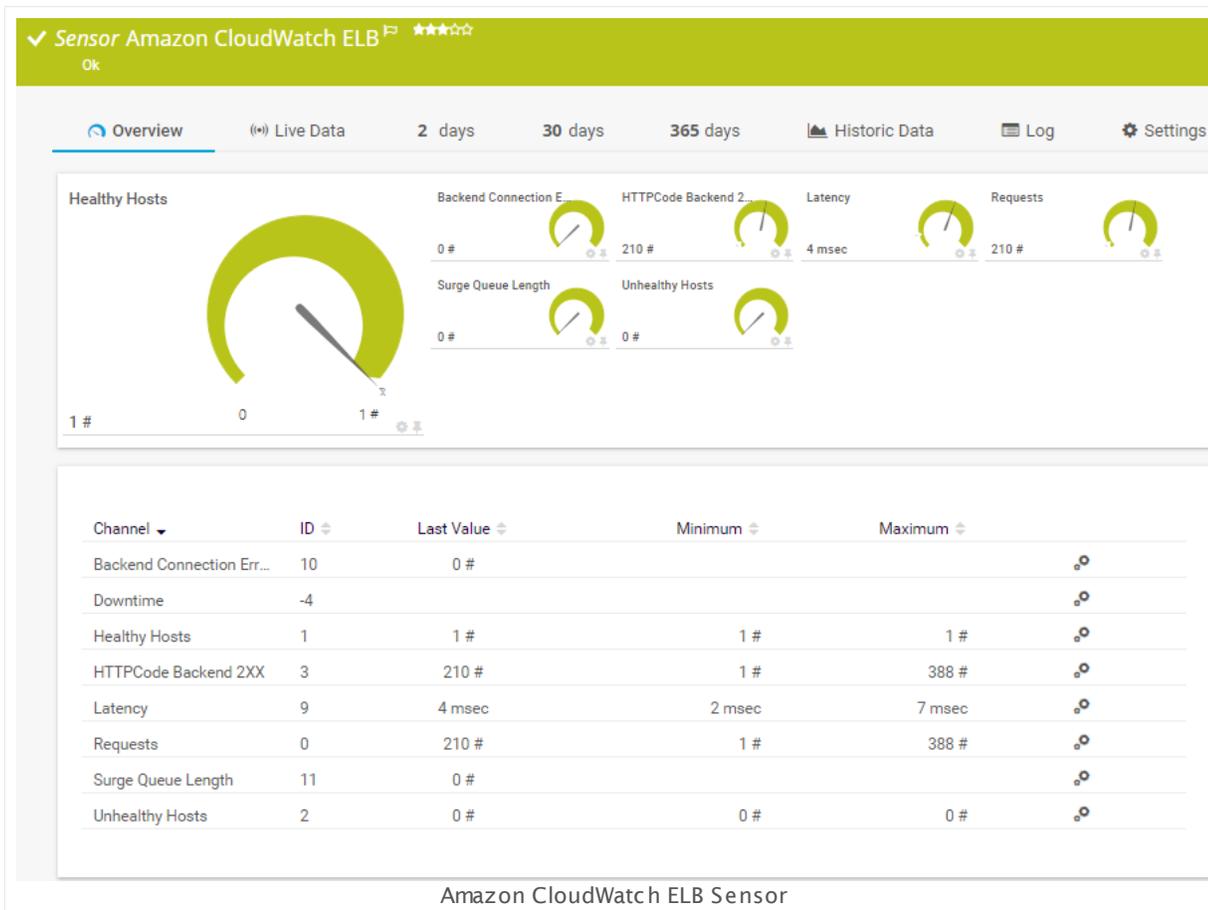
The Amazon CloudWatch ELB sensor monitors the performance of the Amazon Cloud service Elastic Load Balancing (ELB).

The sensor can show the following:

- Host Count
- HTTP Result Count (2xx, 3xx, 4xx, 5xx)
- Latency
- Queue

See [Supported Metrics](#)⁵³⁷ for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
8 Amazon CloudWatch ELB Sensor

- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#)^[3170] with a latency of **0 seconds** to receive all notifications for this sensor (**[...] for at least 0 seconds**).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The [AWS Identity and Access Management \(IAM\)](#) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the [Microsoft .NET Framework](#) to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required [.NET](#) version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the **Load Balancers** or **Availability Zones** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region	<p>Shows the region in which the monitored AWS instance runs. It is one of the following regions:</p> <ul style="list-style-type: none"> ▪ US East (Northern Virginia) ▪ US West (Oregon) ▪ US West (Northern California) ▪ Canada (Central) ▪ EU (Ireland) ▪ EU (London) ▪ EU (Frankfurt) ▪ Asia Pacific (Singapore)
--------	---

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend
-----------------	--

SENSOR DISPLAY

on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

Elastic Load Balancing (ELB)

- RequestCount (Sum)
- SpilloverCount (Sum)
- HealthyHostCount (Minimum)
- UnHealthyHostCount (Maximum)
- BackendConnectionErrors (Sum)
- HTTPCode_Backend_2XX (Sum)
- HTTPCode_Backend_3XX (Sum)
- HTTPCode_Backend_4XX (Sum)
- HTTPCode_Backend_5XX (Sum)
- HTTPCode_ELB_4XX (Sum)
- HTTPCode_ELB_5XX (Sum)
- Latency (Average)
- SurgeQueueLength (Average)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- Elastic Load Balancing (ELB)
- Load Balancer
 - Availability Zone

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.9 Amazon CloudWatch RDS Sensor

The Amazon CloudWatch RDS sensor monitors the performance of the Amazon Cloud service Relational Database Service (RDS).

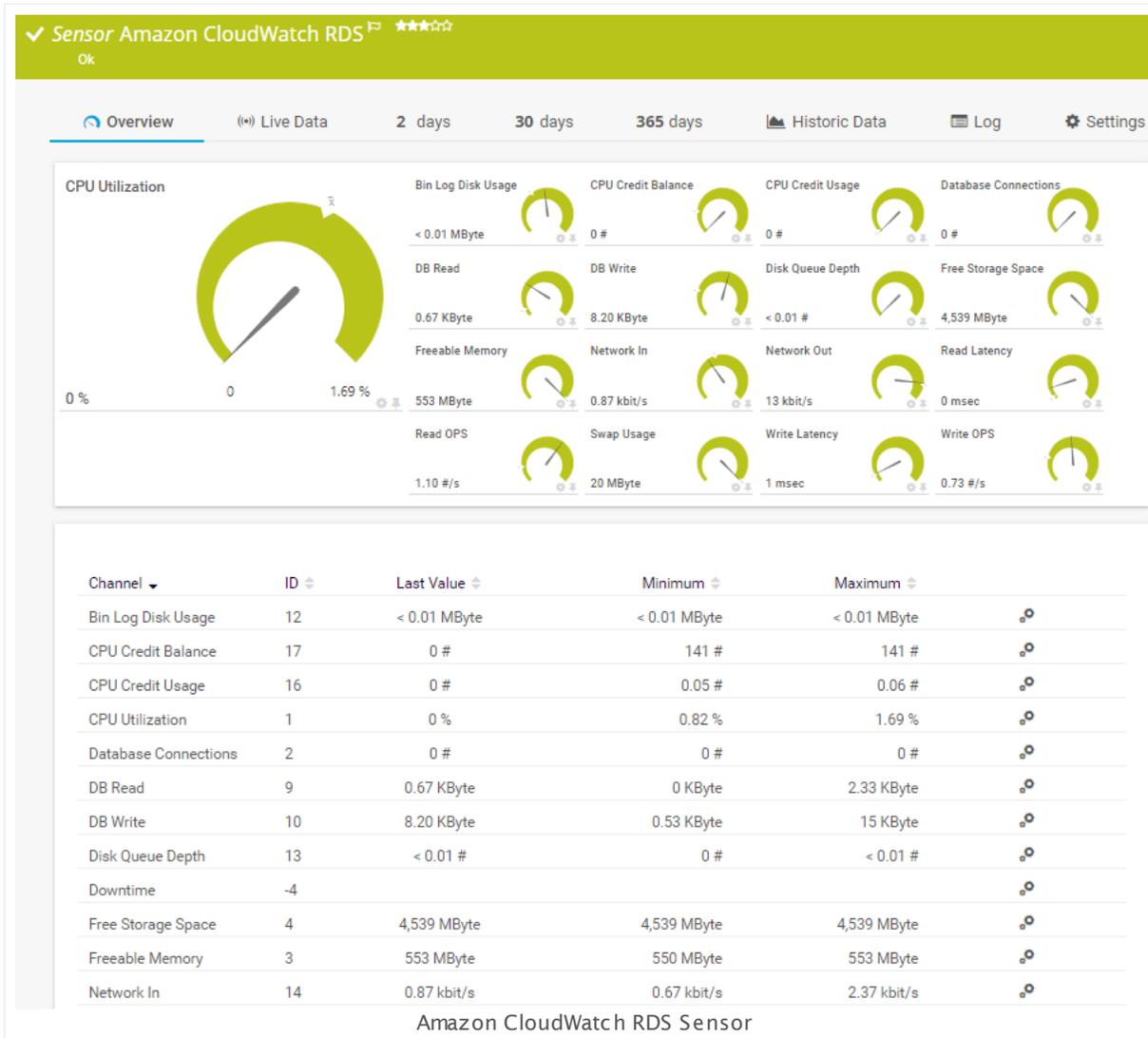
The sensor can show the following:

- CPU Utilization
- CPU Credit Usage and CPU Credit Balance
- Memory Usage
- Database I/O
- Network I/O
- Storage information

See [Supported Metrics](#)⁵⁵⁰ for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 9 Amazon CloudWatch RDS Sensor



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#)^[3170] with a latency of **0 seconds** to receive all notifications for this sensor ([\[...\] for at least 0 seconds](#)).

- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵¹ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the **Engines** or **Database Instances** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3270], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region Shows the region in which the monitored AWS instance runs. It is one of the following regions:

- US East (Northern Virginia)
- US West (Oregon)
- US West (Northern California)
- Canada (Central)
- EU (Ireland)
- EU (London)
- EU (Frankfurt)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

AMAZON CLOUDWATCH SPECIFIC

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📁 For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. ☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- | | |
|-----------------------------------|--|
| Relational Database Service (RDS) | <ul style="list-style-type: none"> ▪ CPUUtilization (Average) ▪ CPUCreditUsage (Average) ▪ CPUCreditBalance (Average) ▪ DatabaseConnections (Sum) ▪ FreeableMemory (Sum) ▪ FreeStorageSpace (Average) ▪ SwapUsage (Sum) ▪ BinLogDiskUsage (Sum) ▪ DiskQueueDepth (Sum) ▪ ReplicLag (Average) ▪ ReadIOPS (Sum) ▪ WriteIOPS (Sum) ▪ ReadLatency (Average) ▪ WriteLatency (Average) ▪ ReadThroughput (Sum) |
|-----------------------------------|--|

AMAZON CLOUDWATCH METRICS

- WriteThroughput (Sum)
- NetworkReceiveThroughput (Sum)
- NetworkTransmitThroughput (Sum)

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- | | |
|-----------------------------------|--|
| Relational Database Service (RDS) | <ul style="list-style-type: none">▪ Engine▪ DB Instance |
|-----------------------------------|--|

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.10 Amazon CloudWatch SNS Sensor

The Amazon CloudWatch SNS sensor monitors the performance of the Amazon Cloud service Simple Notification Service (SNS).

The sensor can show the following:

- Message Counting
- Error Counting

See [Supported Metrics](#)^[562] for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.
- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.

- Configure [notification triggers](#)³¹⁷⁰ with a latency of **0 seconds** to receive all notifications for this sensor ([\[...\] for at least 0 seconds](#)).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region). For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The **AWS Identity and Access Management (IAM)** account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵¹ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

i This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the **Applications**, **Platforms** or **Topics** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

AMAZON CLOUDWATCH SPECIFIC

Region	<p>Shows the region in which the monitored AWS instance runs. It is one of the following regions:</p> <ul style="list-style-type: none">▪ US East (Northern Virginia)▪ US West (Oregon)▪ US West (Northern California)▪ Canada (Central)▪ EU (Ireland)▪ EU (London)▪ EU (Frankfurt)▪ Asia Pacific (Singapore)▪ Asia Pacific (Tokyo)▪ Asia Pacific (Sydney)▪ Asia Pacific (Seoul)▪ Asia Pacific (Mumbai)▪ South America (Sao Paulo)
--------	--

AMAZON CLOUDWATCH SPECIFIC

	Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📖 For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- | | |
|-----------------------------------|---|
| Simple Notification Service (SNS) | <ul style="list-style-type: none"> ▪ NumberOfNotificationsDelivered (Sum) ▪ NumberOfNotificationsFailed (Sum) ▪ NumberOfMessagesPublished (Average) ▪ PublishSize (Average) |
|-----------------------------------|---|

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- | | |
|-----------------------------------|--|
| Simple Notification Service (SNS) | <ul style="list-style-type: none"> ▪ Application ▪ Platform ▪ Application and Platform ▪ Topic |
|-----------------------------------|--|

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.11 Amazon CloudWatch SQS Sensor

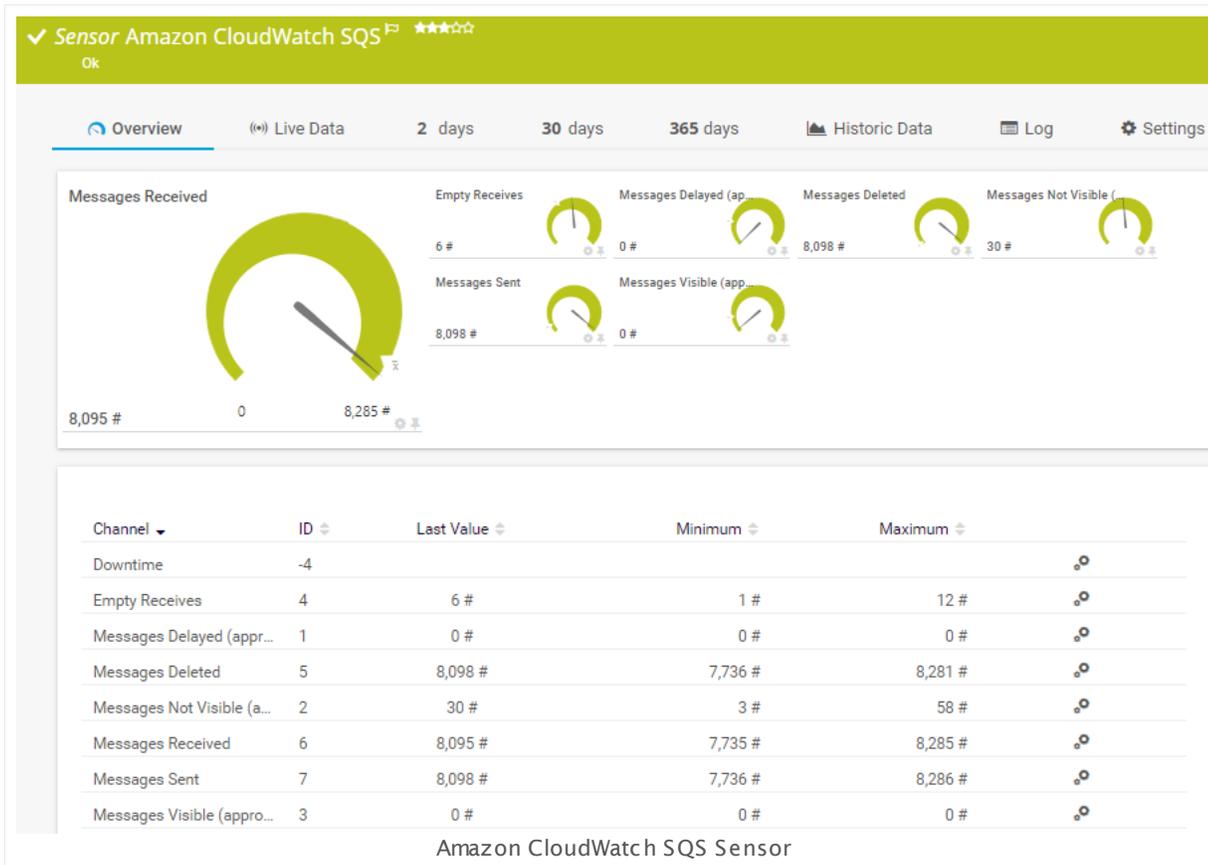
The Amazon CloudWatch SQS sensor monitors the performance of the Amazon Cloud service Simple Queue Service (SQS).

The sensor can show the following:

- Message Counting
- Error Counting
- Delay

See [Supported Metrics](#)⁵⁷⁴ for a list of data that this sensor can potentially show in dedicated channels.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Requires access rights for CloudWatch queries. For details, see the Knowledge Base: [How do I define access rights for Amazon CloudWatch queries?](#)
- Requires .NET 4.5 or higher on the probe system.

- Define [Credentials for Amazon CloudWatch](#)^[415] in settings that are higher in the [Object Hierarchy](#)^[133], for example, in the [parent device settings](#)^[402].
- The minimum scanning interval for this sensor is **15 minutes**.
- Configure [notification triggers](#)^[3170] with a latency of **0 seconds** to receive all notifications for this sensor ([\[...\] for at least 0 seconds](#)).
- This sensor will only show those channels for which it receives data from Amazon. You can check the availability of data in your CloudWatch Console on the AWS website. To know which channels are possible for the various services of this Amazon CloudWatch sensor, see the manual section **Supported Metrics**. If the sensor does not receive data from Amazon for more than 6 hours, it will go into error status.
- To know which dimensions you can monitor, see the manual section **Supported Dimensions**.
- Amazon will charge you (a small amount) for each "Amazon CloudWatch API Request" query the sensor sends to the Amazon servers. Depending on the service, each Amazon CloudWatch sensor sends about 10 to 30 requests with each scanning interval. Last time we checked the Amazon price list, they charged max. US\$ 0.014 per 1,000 requests (depending on your region).
For details, see the Knowledge Base: [How much does Amazon charge for using the CloudWatch API?](#)
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: Access Rights for Amazon CloudWatch Queries

The [AWS Identity and Access Management \(IAM\)](#) account that you use with the Amazon CloudWatch sensor needs specific rights to query any metrics.

 For details, see this Knowledge Base article: [How do I define access rights for Amazon CloudWatch queries?](#)

Requirement: .NET Framework

 This sensor type requires the [Microsoft .NET Framework](#) to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required [.NET](#) version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG looks for available instances.

 This can take up to several minutes.

Select which service instance(s) you want to monitor. PRTG creates one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

AMAZON CLOUDWATCH SPECIFIC

Services Select the **Queues** you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)

BASIC SENSOR SETTINGS



Parent Tags

Shows **Tags** that this sensor inherits from its parent device, group, and probe. This setting is shown for your information only and cannot be changed here.

Tags

Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

AMAZON CLOUDWATCH SPECIFIC

Region

Shows the region in which the monitored AWS instance runs. It is one of the following regions:

- US East (Northern Virginia)
- US West (Oregon)
- US West (Northern California)
- Canada (Central)
- EU (Ireland)
- EU (London)
- EU (Frankfurt)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)

AMAZON CLOUDWATCH SPECIFIC

- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description	Shows the description of the AWS service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID	Shows the ID of the AWS instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Result Handling	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
-----------------	---

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[336] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- ⓘ If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- ⓘ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

ⓘ This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

For Amazon CloudWatch sensors, the minimum scanning interval is **15 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Supported Metrics

AMAZON CLOUDWATCH METRICS

- | | |
|-----------------------------------|--|
| Simple Notification Service (SNS) | <ul style="list-style-type: none"> ▪ <code>SentMessageSize</code> (Sum) ▪ <code>NumberOfMessagesSent</code> (Sum) ▪ <code>NumberOfMessagesReceived</code> (Sum) ▪ <code>NumberOfMessagesDeleted</code> (Sum) ▪ <code>NumberOfEmptyReceives</code> (Sum) ▪ <code>ApproximateNumberOfMessagesVisible</code> (Average) ▪ <code>ApproximateNumberOfMessagesNotVisible</code> (Average) ▪ <code>ApproximateNumberOfMessagesDelayed</code> (Average) |
|-----------------------------------|--|

Supported Dimensions

AMAZON CLOUDWATCH DIMENSIONS

- | | |
|-----------------------------------|--|
| Simple Notification Service (SNS) | <ul style="list-style-type: none"> ▪ <code>Queue</code> |
|-----------------------------------|--|

More

Knowledge Base: How do I define access rights for Amazon CloudWatch queries?

- <https://kb.paessler.com/en/topic/38083>

Knowledge Base: How much does Amazon charge for using the CloudWatch API?

- <https://kb.paessler.com/en/topic/37543>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.12 Business Process Sensor

The Business Process sensor is a powerful and very flexible sensor that allows you to give a summary status of whole business processes while monitoring several process components.

This means that you can create your very own and individual sensor with channels based on data from other sensors ("source sensors") that are specific to your network.

The sensor can show the following:

- The summarized status of the objects contained in each channel according to the individually defined error and warning thresholds
 - The overall and summarized status of all channels in the Global State channel
- ❗ The Business Process sensor does not show values in the "Downtime" channel because they cannot be calculated for this sensor type.
- ❗ If you want to process values from other sensors and you want to perform calculations with these values, for example, use the [Sensor Factory Sensor](#) instead.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum
Downtime	-4			
Global State	0	Inactive	Inactive	Inactive
TEST	1	Inactive	Inactive	Inactive

Business Process Sensor

Sensor in Other Languages

Dutch: **Bedrijfs Proces**, French: **Processus métier**, German: **Business Process**, Japanese: ? ?
? ? ? ? ? ? , Portuguese: **Processo de Negócio**, Russian: **Бизнес-процесс**, Simplified Chinese:

????, Spanish: **Proceso comercial**

Remarks

- Knowledge Base: [How does the Business Process sensor calculate summarized sensor states?](#)
- This sensor [does not support more than 50 channels](#) officially.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).

Limited to 50 Sensor Channels

⚠ PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

BUSINESS PROCESS SPECIFIC SETTINGS

Channel Name	<p>Enter a meaningful name to identify the channel. To add a new channel to the sensor, click the Enter Channel Name field, enter a name for the channel, and confirm with the enter or tab key.</p> <p>i It might take several sensor scans until new channel names or changes to existing channel names become visible.</p>
Error Threshold %	<p>Set a percentage limit to define when the sensor channel displays a Down status. Please enter an integer value. Default is 50%.</p> <p>i This value depends on how many objects you feed into a business process channel.</p> <p>If a channel contains less source objects in "up" condition than the error threshold defines, this channel and the Global State channel of the Business Process sensor will show a Down.</p> <p>The Sensor States^[195] that allow for the "up" condition ▲ of a Business Process channel are the following:</p> <ul style="list-style-type: none">▪ Up▪ Warning▪ Unusual

BUSINESS PROCESS SPECIFIC SETTINGS

- Partial Down

All other sensor states will support the "down" condition ▼ (see the table below).

For example, if you define 4 source sensors for a channel, an error threshold of 50% means that 3 source sensors have to be in "down" condition to set this channel to a **Down** status. So, 50% means that more than half of the source sensors must not be in "up" condition to set the sensor to **Down**.

 For more information, an illustration of the business process mechanisms, and some use cases of the Business Process sensor, see the table [below](#) ^[580] and this Knowledge Base article: [How can I use the Business Process sensor?](#)

Warning Threshold %

Set a percentage limit to define when the sensor channel displays a **Warning** status. Please enter an integer value. Default is **75%**.

 This value depends on how many objects you feed into a business process channel.

If a channel contains less source objects in "up" condition than the threshold defines, this channel and the **Global State** channel of the Business Process sensor will show a **Warning** status (and so the sensor status is **Warning**).

The [Sensor States](#) ^[195] that allow for the "up" condition ▲ of a Business Process channel are the following:

- Up
- Warning
- Unusual
- Partial Down

All other sensor states will support the "down" condition ▼ (see the table below).

For example, if you define 4 source sensors for a channel, a warning threshold of 75% means that all 4 source sensors have to be in "down" condition to set this channel to a **Warning** status. So, 75% means that more than three out of four of the source sensors must not be in "up" condition to set the sensor to **Warning**.

 For more information, an illustration of the business process mechanisms, and some use cases of the Business Process sensor, see the table [below](#) ^[580] and this Knowledge Base article: [How can I use the Business Process sensor?](#)

BUSINESS PROCESS SPECIFIC SETTINGS

Objects

Enter the objects you want to have in a channel using the + sign. This way, you can choose the desired objects from the device tree with the [Object Selector](#)^[240]. You can also start typing the object's ID, name, or a tag. PRTG then suggests the possible objects to be selected.

You can add sensors, devices, groups, and probes to a channel. Each object you add is weighted equally, no matter if it is a single sensor or a whole device with many sensors. To give more weight to a specific object, add it several times. For example, add it twice to give double weight to an object, add it three times to give it triple weight.

 A probe, group, or device is as long in "up" condition  as it does not contain any sensors in "down" condition .

Up and Down Conditions

The **Business Process Up**  and **Down**  **conditions** are different from the normal PRTG up and down [Sensor States](#)^[195]. This is necessary for the Business Process sensor to be able to calculate summarized states and to show a calculated result for a whole business process. This table illustrates which sensor status leads to which Business Process condition.

THE RELATION BETWEEN OBJECT STATES AND BUSINESS PROCESS CONDITIONS

Channel Object Status	Business Process Condition	Reason: Why does a given sensor status correspond to a given Business Process condition?
 Up	Up 	The monitored object works, so everything is fine.
 Warning	Up 	The sensor may show a warning, but the monitored object still works.
 Partial Down	Up 	This status is available in a cluster setup and is displayed if at least one cluster node reports the sensor as up and at least one cluster node reports it as down. With at least one up report, the monitored object is supposed to be working and meets the business process up condition.

THE RELATION BETWEEN OBJECT STATES AND BUSINESS PROCESS CONDITIONS

 Unusual	Up		The sensor may show unusual values, but the monitored object works.
 Collecting	Up		The sensor still waits for more monitoring data to definitely decide about the sensor status, but so far the monitored object works. This PRTG internal status is visualized as Unknown in the PRTG web interface.
 Down	Do wn		The monitored object does not work.
 Unknown	Do wn		The sensor does not know if the monitored object works, for example because it has not yet received any data or because it has not received any data for a certain amount of time.
 None	Do wn		The sensor has not yet received any monitoring data from the monitored object. This PRTG internal status is visualized as Unknown in the PRTG web interface.
 Paused	Do wn		The monitored object does not work and monitoring has been paused, for example actively by the user, by inheritance, or by executed schedules. It might be convenient to exclude regularly or frequently paused objects from your business process monitoring, so you do not give more weight than necessary to a Business Process down status because of issues you already know about.
 Down Acknowledged	Do wn		The monitored object does not work and someone already knows.

 If you encounter issues with your Business Process sensor and want to [contact our support team](#)³⁴²¹, please send us your exact configuration. It helps us find the cause more easily and quickly. Click the little clipboard icon in the upper-right of the **Business Process Specific Settings** table to copy your configuration:

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
12 Business Process Sensor

Business Process Specific Settings

States and Conditions *Step 1. The sensor checks the conditions of the objects in its channels. The following object states allow for the up condition of a channel:*
Up, Warning, Unusual, Partial Down, Unknown (Collecting)

These are the object states that will support the down condition of a channel:
Down, Unknown (None), Paused, Down Acknowledged

Have a look at the manual if you are interested in the reasoning behind these decisions. A probe, group, or device that you add to a channel is in up condition as long as none of its sensors are in down condition.

Step 2. The Business Process sensor compares your thresholds with the conditions of the objects in a channel to check if the channel is in an all-over up, warning, or down status. If there is a smaller percentage of up objects than indicated by your warning or error threshold, the channel status will be set to warning or down respectively.

Channel Name	Error	Warning	Objects
Test	50	75	
Enter Channel Name	50	75	

The Business Process Sensor Configuration Clipboard

You find your configuration in the window that opens. Copy the marked text and paste it into the [support form](#)³⁴²⁴ to send it our support team.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How does the Business Process sensor calculate summarized sensor states?

- <https://kb.paessler.com/en/topic/66647>

Knowledge Base: How can I use the Business Process sensor?

- <https://kb.paessler.com/en/topic/67109>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.13 Cisco IP SLA Sensor

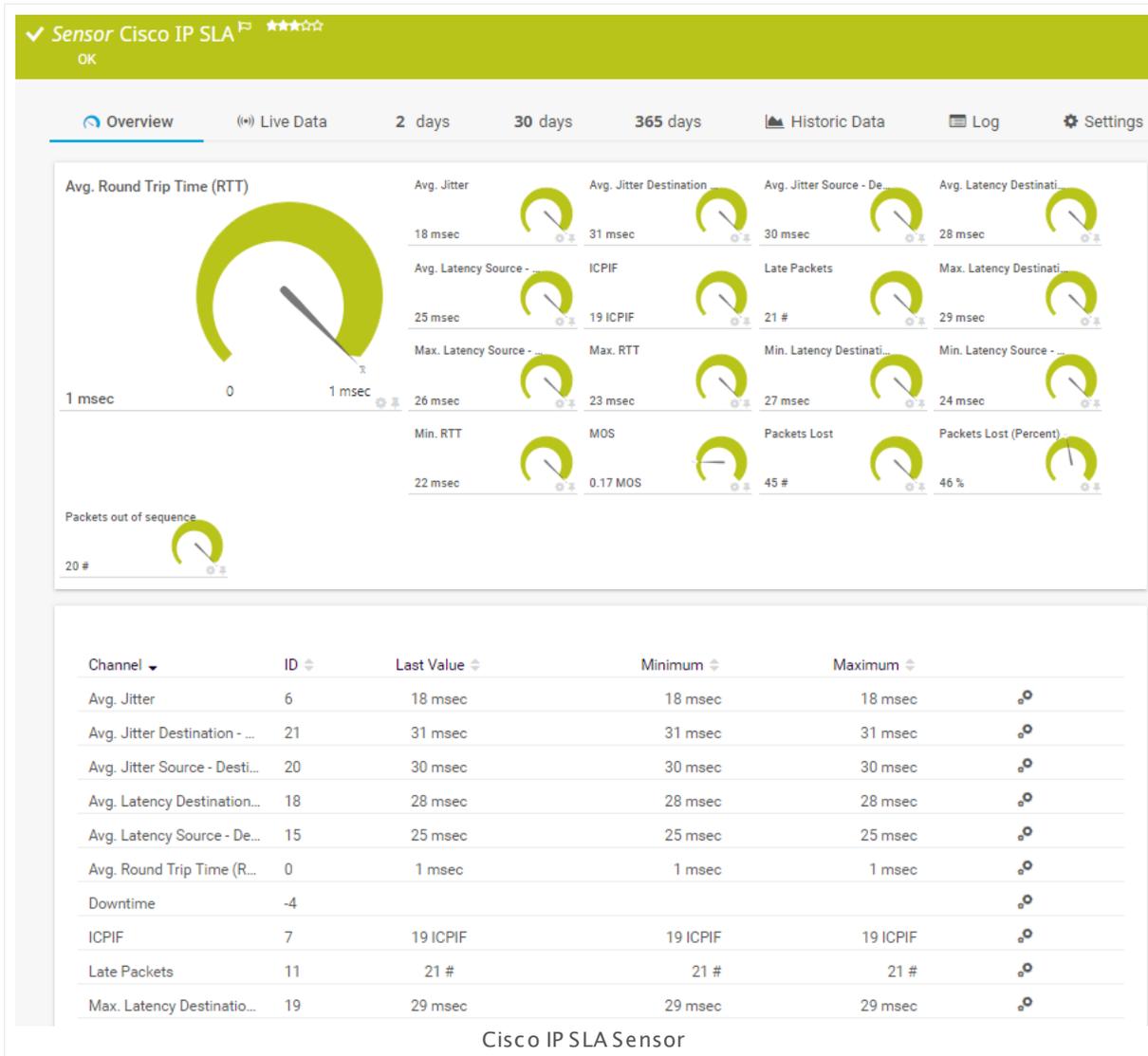
The Cisco IP SLA sensor monitors Voice over IP (VoIP) network parameters using IP Service Level Agreement (SLA) from Cisco via Simple Network Management Protocol (SNMP).

It shows different aspects provided by the queried device:

- Average, maximum, and minimum Round Trip Time (RTT)
- Average jitter
- Average jitter from source to destination and vice versa
- Average latency from source to destination and vice versa
- Impairment Calculated Planning Impairment Factor (ICPIF)
- Late packets in percent
- Average, maximum, and minimum latency from source to destination and vice versa
- Mean Opinion Score (MOS)
- Number of lost packets and in percent
- Packets out of sequence in percent
- Sense code (status code of RTT entry)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 13 Cisco IP SLA Sensor



Remarks

- For a general introduction to the technology behind Quality of Service monitoring, please see manual section [Monitoring Quality of Service](#).
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which SLAs you want to monitor. PRTG creates one sensor for each SLA you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IP SLA SPECIFIC

IP SLAs

Select the IP SLAs you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The list options depend on the configuration of the queried device. If you miss a type here, please check the configuration of your target device. PRTG can support the following operations with the given type IDs:

- **echo** (1)
- **pathEcho** (2)
- **fileIO** (3)
- **script** (4)
- **udpEcho** (5)
- **tcpConnect** (6)
- **http** (7)
- **dns** (8)
- **jitter** (9)
- **dls** (10)
- **dhcp** (11)
- **ftp** (12)
- **icmp-jitter** (16)
- **path-jitter** (23)

 The numbers above are the IDs of the SLA types as reported by the target device. PRTG translates them into the corresponding strings. These IDs are independent from the IDs that you see in the first column of the list. If the target device returns other values than given above, the sensor will show an error message that it cannot find the type.

IP SLA SPECIFIC

- Packet Loss values are summarized, but have no explicit channel for Source—Destination or Destination—Source values.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IP SLA SPECIFIC

ID

Type

Name (Tag)

Owner

Frequency

These fields show SLA specific settings that the queried SLA device provides. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.14 Citrix XenServer Host Sensor

The Citrix XenServer Host sensor monitors a Xen host server via Hypertext Transfer Protocol (HTTP).

It can show the following:

- CPU usage
- Memory usage (free, used, allocation)
- Network usage
- Number of running virtual machines
- Load average

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: Citrix XenServer Host, French: Hôte Citrix XenServer, German: Citrix XenServer Host, Japanese: Citrix XenServer, Portuguese: Citrix XenServer Host, Russian: Узел Citrix XenServer, Simplified Chinese: Citrix XenServer, Spanish: Citrix XenServer Host

Remarks

- The parent device must be a Citrix XenServer version 5.0 or later.
- The parent device has to represent one host server of your XenServer pool.
- Requires credentials for Xen servers to be defined for the device you want to use the sensor on.
- Requires .NET 4.5 or later on the probe system.
- This sensor type does not fully support TLS 1.2 connections and cannot be added to XenServers with security protocol setting "TLS 1.2 only".
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents **one** host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host.

- ❗ In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Requirement: .NET Framework

✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

- 🧠 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which XenServer hosts you want to monitor. PRTG creates one sensor for each host you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HOST SETTINGS

Host Select the hosts you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) [402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) [181], as well as in [alarms](#) [219], [logs](#) [228], [notifications](#) [3216], [reports](#) [3252], [maps](#) [3278], [libraries](#) [3235], and [tickets](#) [230].

Parent Tags Shows [Tags](#) [139] that this sensor [inherits](#) [140] from its [parent device, group, and probe](#) [133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) [139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) [140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HOST SETTINGS

UUID Shows the Universally Unique Identifier (UUID) of the host that this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

Name Shows the name of the host that this sensor monitors.
Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Knowledge Base: Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
14 Citrix XenServer Host Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

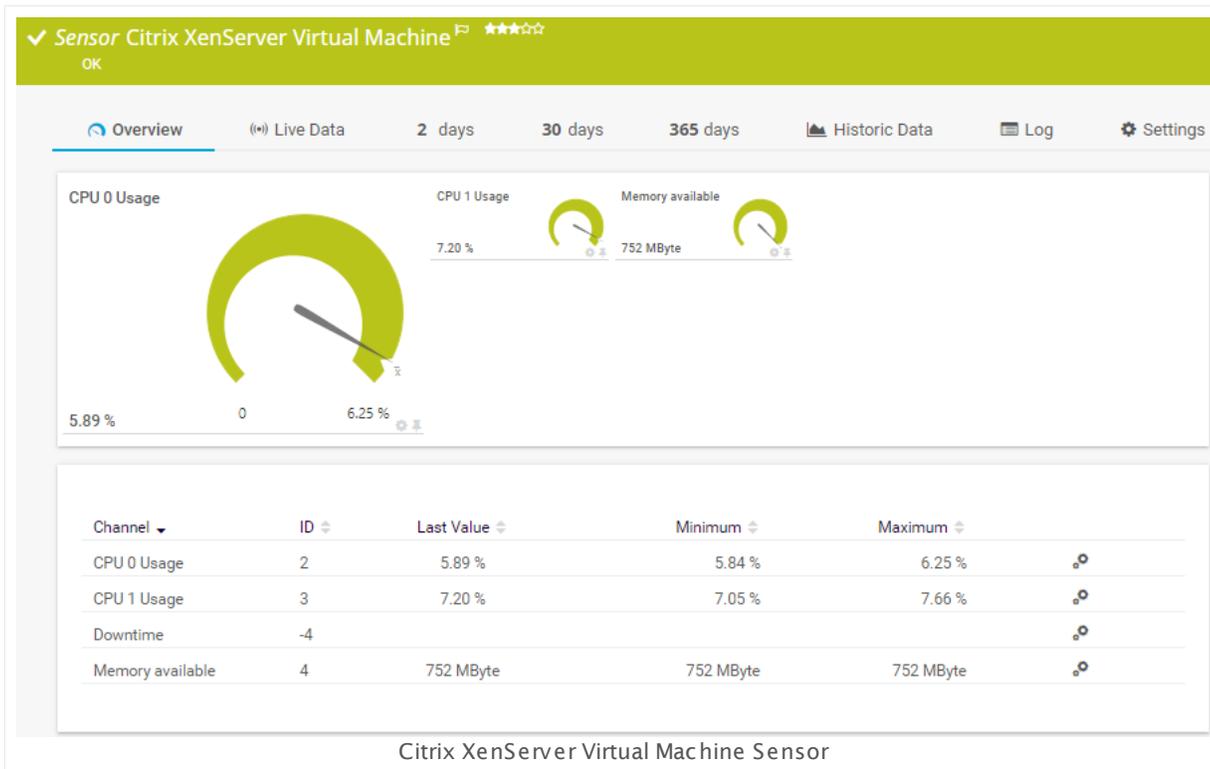
7.8.15 Citrix XenServer Virtual Machine Sensor

The Citrix XenServer Virtual Machine sensor monitors a virtual machine on a Xen server via Hypertext Transfer Protocol (HTTP).

It can show the following:

- CPU usage
- Memory usage (available, used)
- Disk usage (reads and writes per second)
- Network usage (bytes received and sent)
- Balloon driver target size

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Citrix XenServer Virtuelle Machine**, French: **Machine virtuelle Citrix XenServer**, German: **Citrix XenServer Virtuelle Maschine**, Japanese: **Citrix Xen? ? ? ? ? ? ? ?**, Portuguese: **Citrix XenServer Máquina virtual**, Russian: **Виртуальная машина Citrix XenServer**, Simplified Chinese: **Citrix XenServer ? ? ?**, Spanish: **Máquina virtual Citrix XenServer**

Remarks

- The parent device must be a Citrix XenServer version 5.0 or later.
- The parent device has to represent one host server of your XenServer pool.
- Requires credentials for Xen servers to be defined for the device you want to use the sensor on.
- Requires .NET 4.5 or later on the probe system.
- This sensor type does not fully support TLS 1.2 connections and cannot be added to XenServers with security protocol setting "TLS 1.2 only".
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Monitoring a XenServer Pool

In a XenServer pool there is one "pool master" that manages the pool. Incoming queries on any host are automatically forwarded to the pool master. If you want to monitor your virtual machines, or host servers, simply create respective sensors on a device that represents **one** host server of your pool. Internal processes will make sure that monitoring will take place and continue independently from the physical host.

- ❗ In PRTG's device tree, the sensors for virtual machines will always remain on the host you originally created it on, also if it is currently running on a different host.

Requirement: .NET Framework

✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

- 💡 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- ❗ PRTG requests a full list of all virtual machines configured on the Xen server. Therefore, it may take a few seconds before the dialog is loaded.

Select which virtual machines you want to monitor. PRTG creates one sensor for each virtual machine you select in the **Add Sensor** dialog. The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine Select the Virtual Machines (VM) you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) ^[181], as well as in [alarms](#) ^[219], [logs](#) ^[228], [notifications](#) ^[3216], [reports](#) ^[3252], [maps](#) ^[3278], [libraries](#) ^[3235], and [tickets](#) ^[230].

Parent Tags Shows [Tags](#) ^[139] that this sensor [inherits](#) ^[140] from its [parent device, group, and probe](#) ^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) ^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) ^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VIRTUAL MACHINE SETTINGS

UUID Shows the Universally Unique Identifier (UUID) of the virtual machine. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

Name Shows the name of the virtual machine. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Knowledge Base: Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

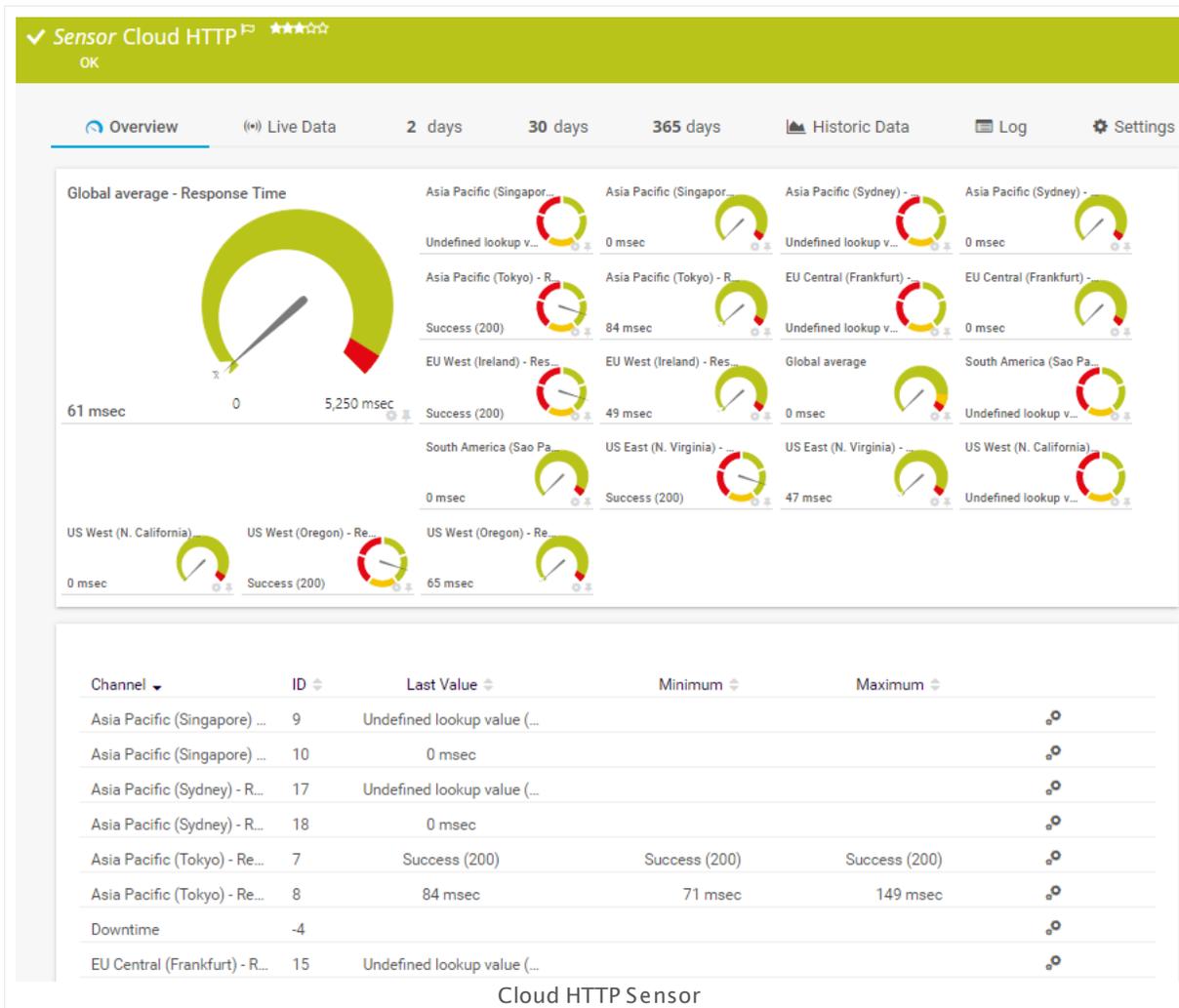
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.16 Cloud HTTP Sensor

The Cloud HTTP sensor monitors the loading time of a web server via Hypertext Transfer Protocol (HTTP) from different locations worldwide using the PRTG Cloud. The locations are distributed over three continents around the globe.

The sensor can show **response time** and **response code** of the target server monitored from the following locations:

- Asia Pacific: Tokyo
- EU West: Ireland
- US East: Northern Virginia
- US West: Oregon
- Global average response time



Sensor in Other Languages

Dutch: **Cloud HTTP**, French: **Cloud HTTP**, German: **Cloud HTTP**, Japanese: ? ? ? ? HTTP, Portuguese: **Cloud HTTP**, Russian: **Облако HTTP**, Simplified Chinese: ? HTTP, Spanish: **Htt p de nube**

Remarks

- The server on which the [PRTG probe](#)^[134] with this sensor runs must have access to the internet. The probe system needs to be able to reach <https://api.prtgcloud.com:443> to communicate with the PRTG Cloud.
- The address you define in the [parent device settings](#)^[402] must be reachable over the internet. You cannot use this sensor to monitor localhost (127.0.0.1) or other target devices that are only reachable within your private network.
- This sensor type does not support IPv6.
- Knowledge Base: [Are there any limits for using Cloud Ping and Cloud HTTP sensors?](#)
- Knowledge Base: [What is the PRTG Cloud Bot?](#)
- This sensor type inherits [Proxy Settings for HTTP Sensors](#)^[419] from the parent device.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)^[3180].
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SETTINGS

URL	<p>Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the IP address/DNS name setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time.</p> <p>PRTG uses a smart URL replacement that allows you to use the parent device's IP address or DNS name setting as part of the URL.</p> <p> For more information, see section Smart URL Replacement below.</p>
Request Method	Choose an HTTP request method to determine how the sensor will request the given URL.

HTTP SETTINGS

- **GET:** Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST:** Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.
- **HEAD:** Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata

This field is only visible when you select the **POST Request Method** setting above. Enter the data part for the POST request here.

 No XML is allowed here!

Timeout (Sec.)

Enter a timeout in seconds for the server request. If the reply takes longer than this value defines, the PRTG will cancel the request and shows an error message. The maximum timeout value is **5** seconds.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- ⓘ If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- ⓘ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

ⓘ This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

For Cloud HTTP sensors, the minimum scanning interval is **10 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

ⓘ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

ⓘ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p> To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- User Group Access
- Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:
- **Inherited:** Use the access rights settings of the parent object.
 - **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
 - **Read:** Users in this group can see the object and review its monitoring results.
 - **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
 - **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)

- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?

- <https://kb.paessler.com/en/topic/63590>

Knowledge Base: What is the PRTG Cloud Bot?

- <https://kb.paessler.com/en/topic/65719>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

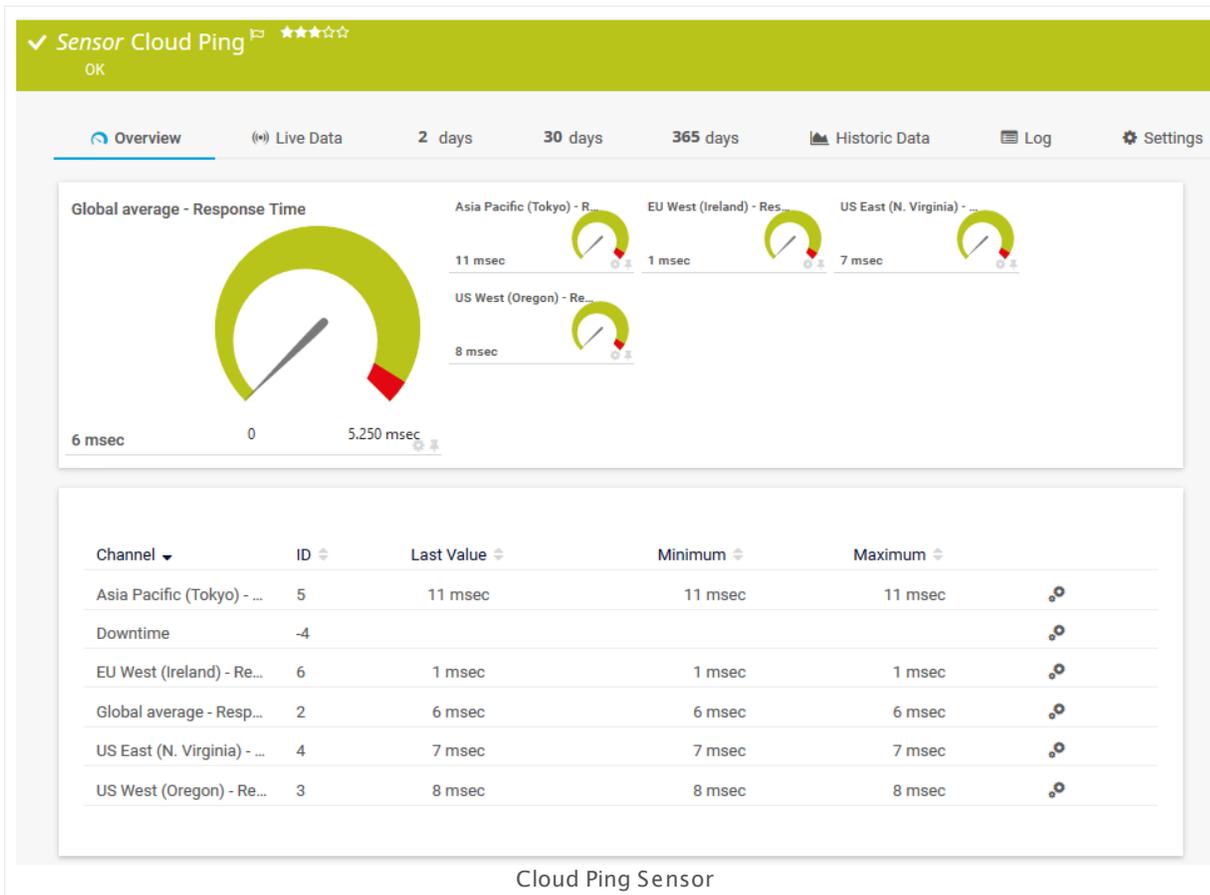
For more general information about settings, see the [Object Settings](#)²¹⁷¹ section.

7.8.17 Cloud Ping Sensor

The Cloud Ping sensor monitors the Transport Control Protocol (TCP) ping times to its parent device from different locations worldwide using the PRTG Cloud. These locations are distributed over three continents around the globe.

The sensor can show the **response times** of the target server pinged from the following locations:

- Asia Pacific: Tokyo
- EU West: Ireland
- US East: Northern Virginia
- US West: Oregon
- Global average response time



Sensor in Other Languages

Dutch: **Cloud Ping**, French: **Cloud Ping**, German: **Cloud Ping**, Japanese: ? ? ? ? Ping,
Portuguese: **Cloud Ping**, Russian: **Пинг из облака**, Simplified Chinese: ? Ping, Spanish: **Ping de nube**

Remarks

- The server on which the [PRTG probe](#) with this sensor runs must have access to the internet. The probe system needs to be able to reach <https://api.prtgcloud.com:443> to communicate with the PRTG Cloud.
- The address you define in the [parent device settings](#) must be reachable over the internet. You cannot use this sensor to monitor localhost (127.0.0.1) or other target devices that are only reachable within your private network.
- This sensor type does not support IPv6.
- Knowledge Base: [Are there any limits for using Cloud Ping and Cloud HTTP sensors?](#)
- Knowledge Base: [What is the PRTG Cloud Bot?](#)
- This sensor type inherits [Proxy Settings for HTTP Sensors](#) from the parent device.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

PING SETTINGS

Packet Size (Bytes)	<p>Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000. We recommend that you use the default value.</p>
Ping Count	<p>Enter the number of Pings to be sent in a row to the parent device with one scan. Please enter an integer value. The default value is 1, the maximum supported ping count is 5.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the PRTG will cancel the request and shows an error message. The maximum timeout value is 5 seconds.</p>
Port	<p>Enter the number of the port that the sensor uses for TCP ping. The default port is 80.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

For Cloud Ping sensors, the minimum scanning interval is **10 minutes**.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Are there any limits for using Cloud Ping and Cloud HTTP sensors?

- <https://kb.paessler.com/en/topic/63590>

Knowledge Base: What is the PRTG Cloud Bot?

- <https://kb.paessler.com/en/topic/65719>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

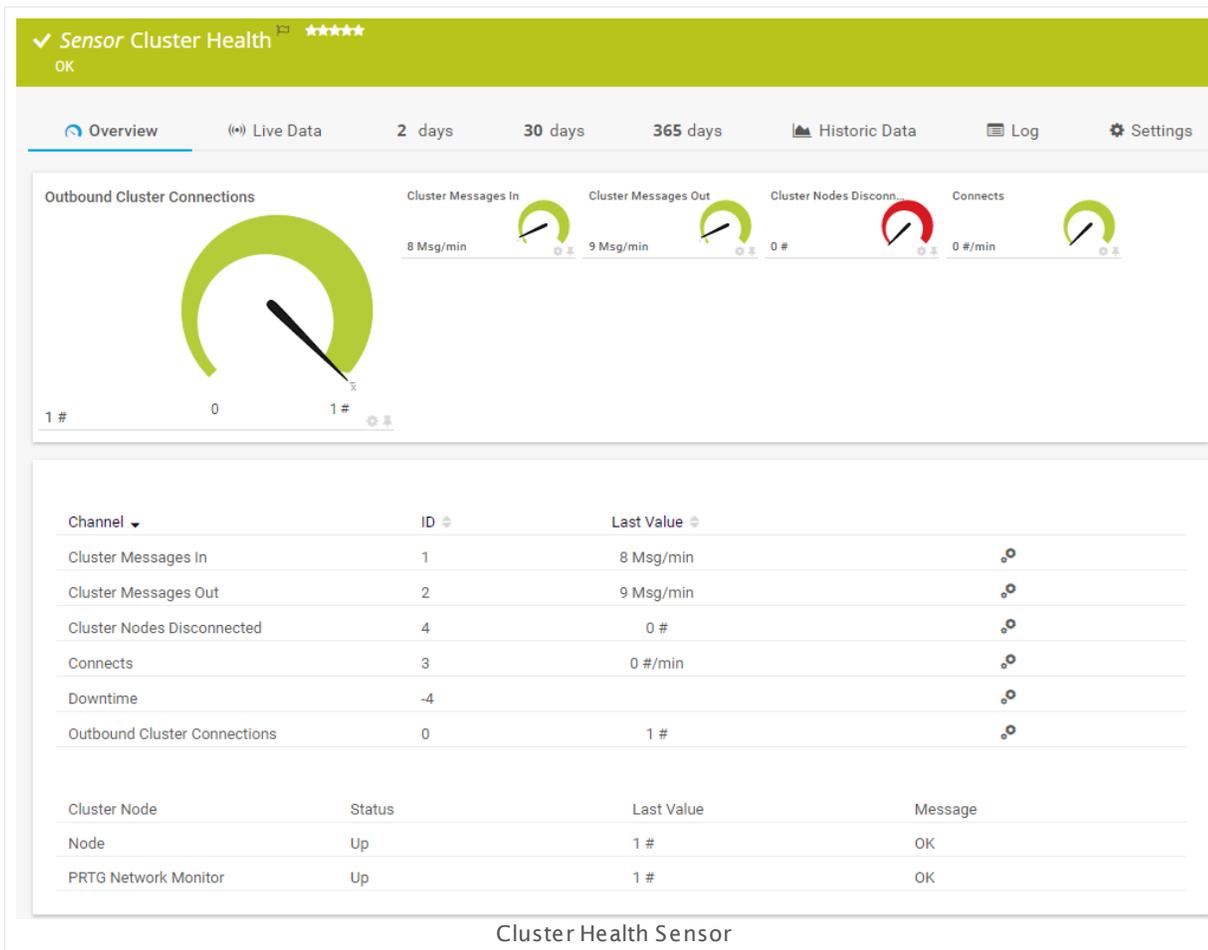
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.18 Cluster Health Sensor

The Cluster Health sensor monitors the health of a [PRTG cluster](#) and indicates the PRTG own system health status.

It measures various internal system parameters of the cluster system:

- Number of connects per minute
- Cluster ingoing and outgoing messages per minute
- Number of connected and disconnected cluster nodes.



Sensor in Other Languages

Dutch: **Cluster Status**, French: **État du cluster**, German: **Cluster-Zustand**, Japanese: クラスターヘルス, Portuguese: **Funcionamento do cluster**, Russian: **Работоспособность кластера**, Simplified Chinese: ? ? ? ? ? , Spanish: **Salud de clúster**

Remarks

- PRTG creates this sensor automatically with a cluster installation. You cannot delete or add it manually.
- If at least one cluster node is disconnected, this sensor will show a **Down status** by default.
- You can review the states of each cluster node on the sensor's **Overview** tab .
- You can choose the cluster member of which you want to show data (or of all nodes) on the **monitoring data review tabs**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the **Device Settings** for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
-  Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
-  If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
-  If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- User Group Access
- Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:
- **Inherited:** Use the access rights settings of the parent object.
 - **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
 - **Read:** Users in this group can see the object and review its monitoring results.
 - **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
 - **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

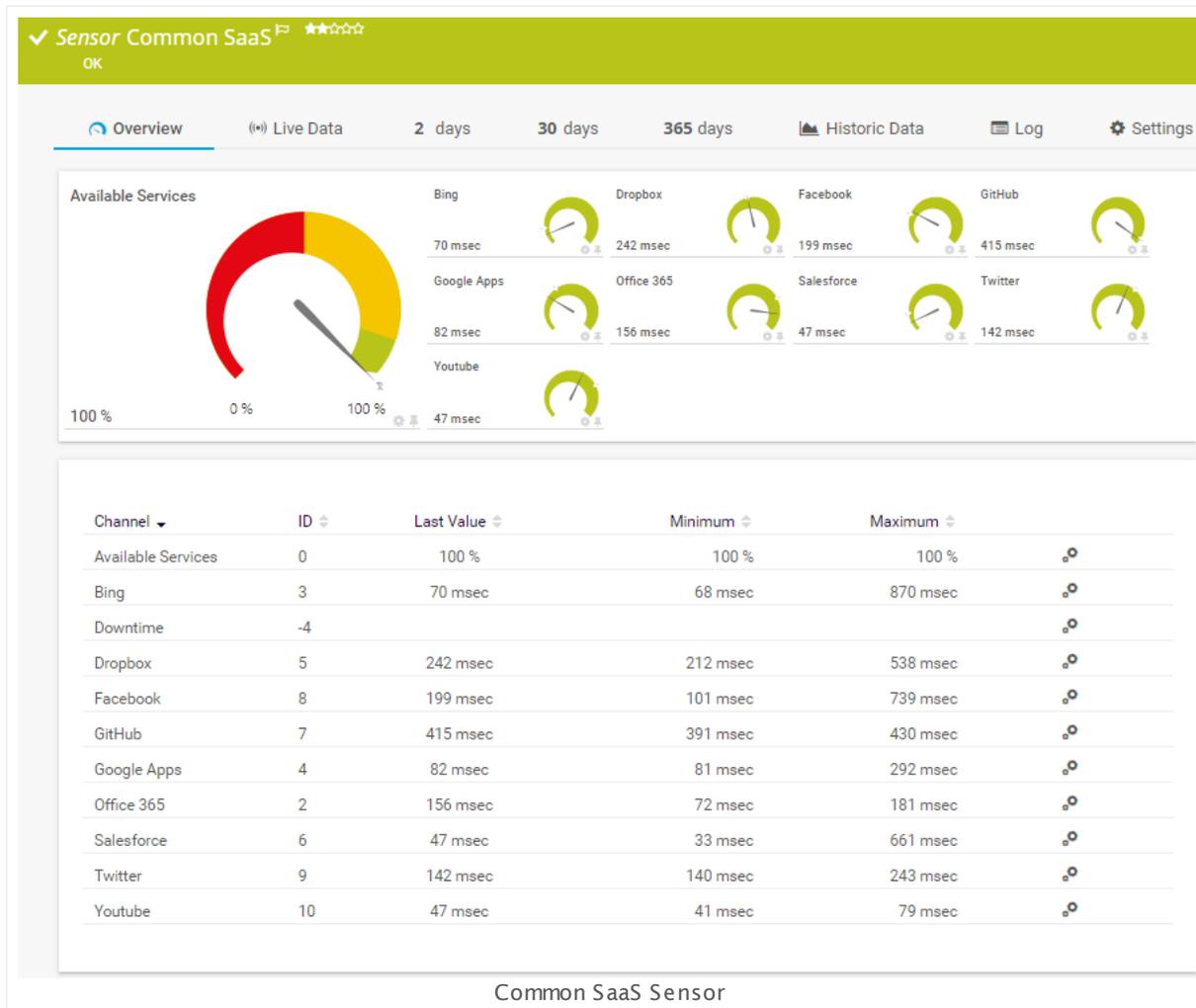
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.19 Common SaaS Sensor

The Common SaaS sensor monitors the availability of several Software as a Service (SaaS) providers. Because your business processes depend more and more on cloud hosts, this sensor type is an important pillar for unified monitoring. With this sensor you can get alarms if your cloud services are not reachable anymore.

This sensor shows the following:

- Available services in percent
- Response times of the following SaaS providers:
 - Bing
 - Dropbox
 - Facebook
 - GitHub
 - Google Apps
 - Office 365
 - Salesforce
 - Twitter
 - Youtube



Sensor in Other Languages

Dutch: **Algemene SaaS**, French: **SaaS courants**, German: **Verbreitete SaaS-Dienste**, Japanese: **Common SaaS**, Portuguese: **Provedores SaaS Comuns**, Russian: **Общий для SaaS**, Simplified Chinese: **?? SaaS**, Spanish: **SaaS común**

Remarks

- The server where the PRTG probe with this sensor runs must have access to the internet.
- PRTG creates this sensor automatically on every new probe device. If the system running the probe has no connection to the internet, please [pause](#)^[245] or [delete](#)^[259] this sensor manually to avoid error messages.
- This sensor type has a fixed scanning interval (15 minutes). You cannot change it.
- This sensor type inherits [Proxy Settings for HTTP Sensors](#)^[419] from the parent device.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)^[3160].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which SaaS providers you want to monitor. The sensor will create one channel for each service you choose in the **Add Sensor** dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

COMMON SAAS SPECIFIC

SaaS Checklist	Select the services you want to monitor with this sensor. You see a list with the names of all items that are available to monitor. Select the desired items by adding check marks in front of the respective lines. The sensor creates one channel for each selection. You can also select and deselect all items by using the check box in the table head.
----------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[213] , logs ^[228] , notifications ^[3216] , reports ^[3262] , maps ^[3270] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result**: Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

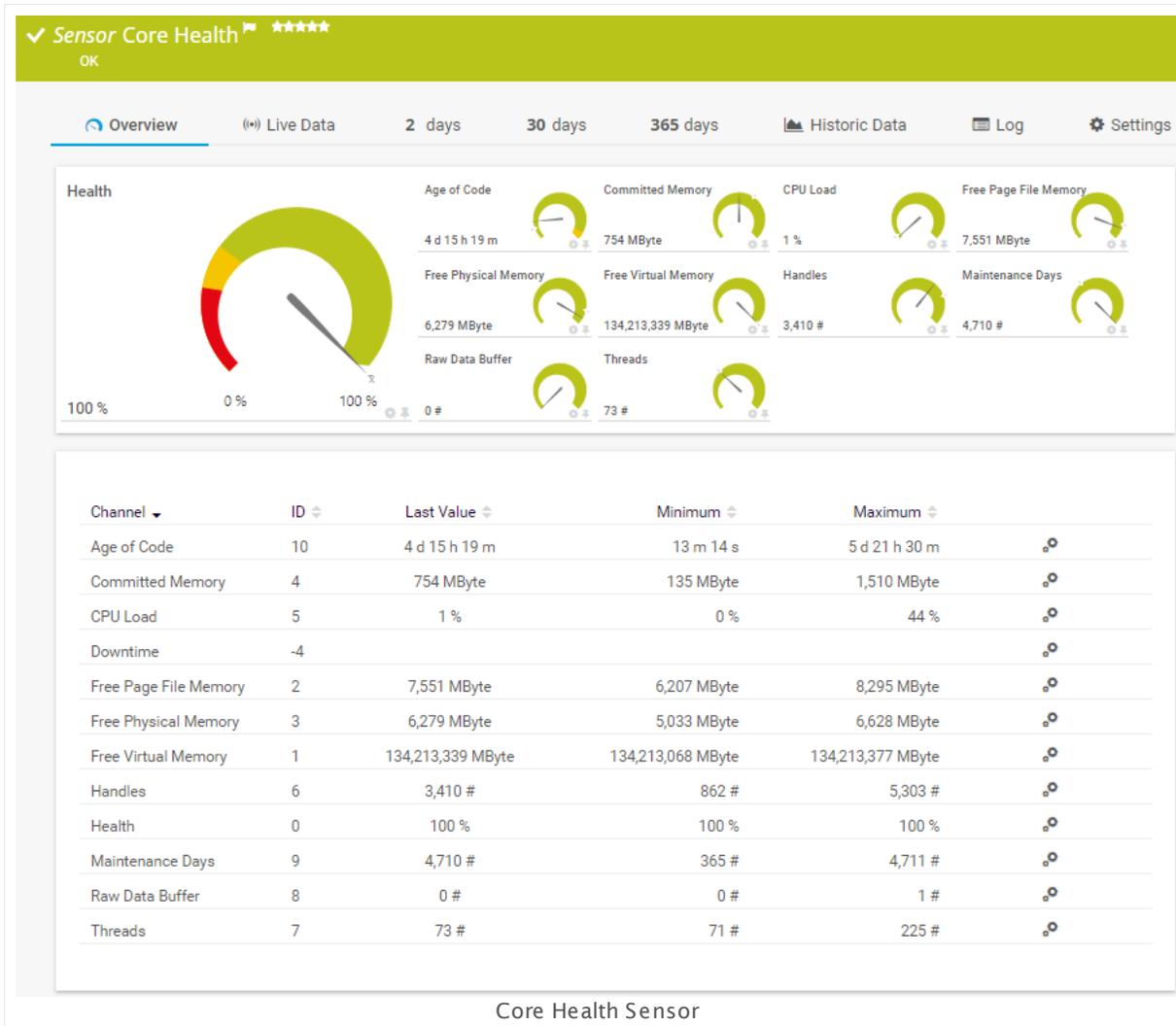
7.8.20 Core Health Sensor

The Core Health sensor monitors internal PRTG parameters. It shows the status of the PRTG core server.

This sensor type checks various parameters of your PRTG core that have an impact on the stability of the system:

- **Health:** This index value sums up the core state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Age of Code:** This channel shows the time that has passed since the last update of your PRTG installation. Please update regularly to get best security and stability for PRTG, as well as the latest features. We recommend that you use the PRTG [Auto-Update](#) 3407 to get new versions automatically.
- **CPU Load:** This channel shows the current percentage CPU load. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.
- **Handles:** This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- **Committed Memory:** This channel shows the amount of memory committed to the PRTG core server as reported by the memory manager.
- **Free Page File Memory:** This channel shows the amount of free page file memory currently available on the system. Page file memory is aggregated RAM and the size of page file. It is the maximum amount of memory that is available on the system to be used for all currently running processes. If it gets too low the system can crash, at least some applications will throw "Out of memory" errors.
- **Free Physical Memory:** This channel shows the amount of free physical memory currently available on the system. This is the RAM that is physically built into the computer. If it gets too low the system will become very slow and PRTG is not usable in a reasonable way anymore. It can happen that some sensors will not be displayed correctly in that case, they will appear disabled (grayed out).
- **Free Virtual Memory:** This channel shows the accessible address space on the system for PRTG. PRTG cannot use more memory than reported here, independently from free page file and physical memory. On a 32-bit OS (operating system) the maximum is 2 GB (3 GB with special settings under Windows); on a 64-bit OS it is 4 GB if PRTG is running as 32-bit version, and unlimited as 64-bit version (only Core). If free virtual memory gets too low, PRTG will throw "Out of memory" errors or the message "not enough storage to process this command" (visible in the Core log).
- **Maintenance Days:** This channel shows the remaining maintenance days of your PRTG on premises license. Please renew your maintenance on time to be sure to get updates for your PRTG on premises installation. PRTG hosted by Paessler instances show a fixed value here for technical reasons.
- **Threads:** This channel shows the number of program parts that are currently running simultaneously. This number can increase with heavy load. The number should not exceed 100 in normal operation.

- **Raw Data Buffer:** This channel shows how much raw data is temporarily stored on the physical memory while I/O operations on the disk. Usually, this value should be 0 (or very low). Investigate increasing values.



Sensor in Other Languages

Dutch: **Core Status**, French: **État du serveur principal**, German: **Serverzustand**, Japanese: ? ? ? ? , Portuguese: **Funcionamento do núcleo**, Russian: **Работоспособность базового сервера**, Simplified Chinese: ? ? ? ? ? , Spanish: **Salud de núcleo**

Remarks

- PRTG creates this sensor automatically and you cannot delete it.
- You can set up this sensor only on a Local Probe device!
- You can find PRTG core system memory related information also in the [PRTG System Status](#) ³³⁹⁹. For details, see the Knowledge Base: [What do the PRTG core system memory parameters mean?](#)

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What do the PRTG core system parameters mean?

- <https://kb.paessler.com/en/topic/71671>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

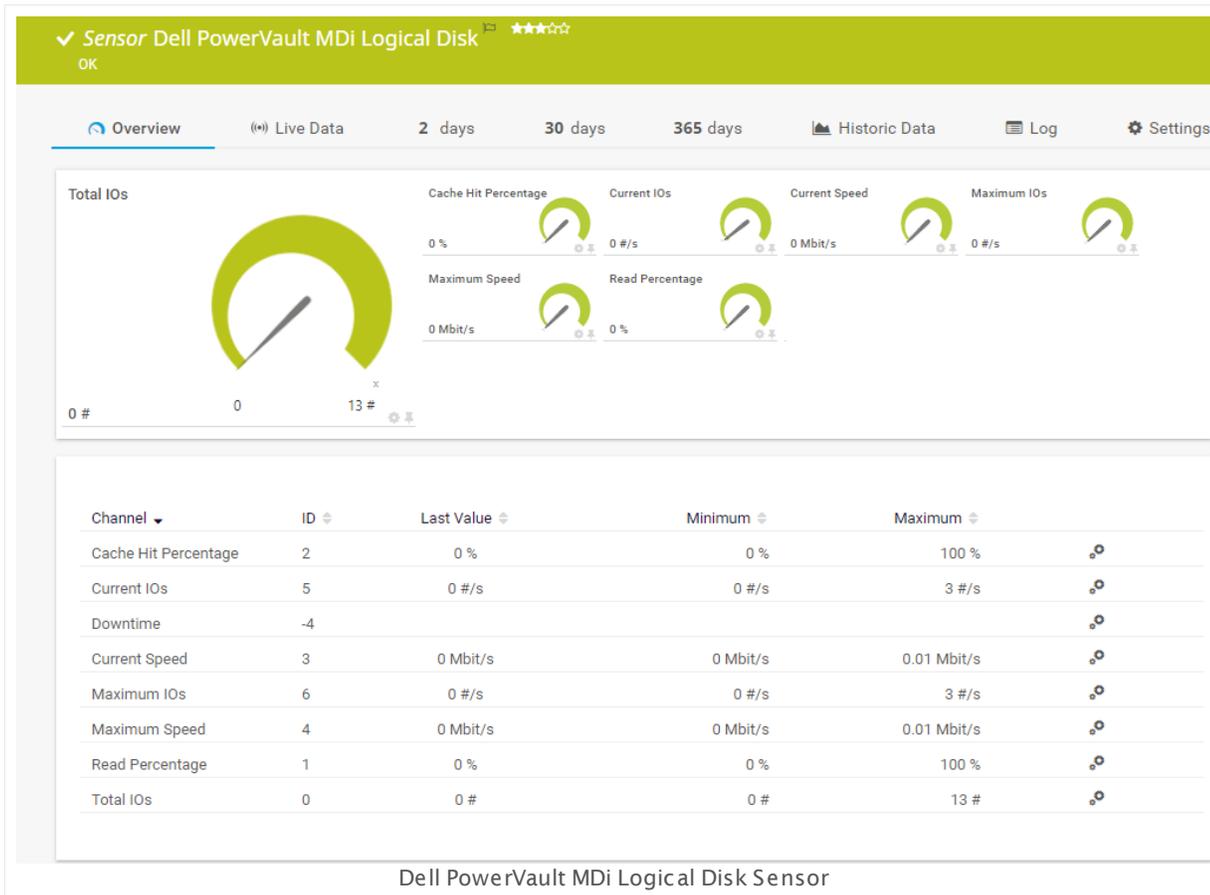
7.8.21 Dell PowerVault MDi Logical Disk Sensor

The Dell PowerVault MDi Logical Disk sensor monitors a virtual disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i. It might work with other models, too.

This sensor can show the following:

- Total number of I/O operations
- Number of current and maximum I/O operations per second
- Current and maximum disk speed
- Read and cache hit percentages

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Dell PowerVault MDi Log. Schijf**, French: **Disque logique Dell PowerVault MDi**, German: **Dell PowerVault MDi Log. Datenträger**, Japanese: **Dell PowerVault MDi ? ? ? ? ?**, Portuguese: **Dell PowerVault MDi Disco Lógico**, Russian: **Лог. диск Dell PowerVault**

MDi, Simplified Chinese: Dell PowerVault MDi ? ? ? ? , Spanish: **Disco de registro de Dell PowerVault MDi**

Remarks

- Works with Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i, and might support other models.
 - **Requires** ⁶⁶⁰ Dell Modular Disk Storage Manager on the probe system. See the Knowledge Base: [Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?](#)
 - Needs the IP address of the Storage Area Network (SAN) defined in the parent device settings.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Dell Modular Disk Storage Manager

 This sensor requires the installation of the **Dell Modular Disk Storage Manager** program. You have to install it on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰. For details about setup, please see **More** section below.

 Create this sensor on a device that has the SAN's IP address configured in the **IP Address/DNS Name** field of the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select which virtual disks you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Virtual Disks

Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Virtual Disk	Shows the name of the virtual disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📁 For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> 📘 This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- <https://kb.paessler.com/en/topic/38743>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.22 Dell PowerVault MDi Physical Disk Sensor

The Dell PowerVault MDi Physical Disk sensor monitors a physical disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, or MD3620f. It might work with other models, too.

This sensor can show following:

- **Mode** of the physical disk
- **Status** of the physical disk

The sensor shows these channels as reported in the **Modular Disk Storage Manager**. Status and mode combined indicate the particular status of a RAID controller physical disk. The table below provides you with the status description according to the Dell documentation:

"STATUS" CHANNEL	"MODE" CHANNEL	DESCRIPTION
Optimal (status: up)	Unassigned (status: up)	The physical disk in the indicated slot is unused and available to be configured.
	Assigned (status: up)	The physical disk in the indicated slot is configured as part of a disk group.
	Hot Spare Standby (status: up)	The physical disk in the indicated slot is configured as a hot spare.
	Hot Spare In Use (status: up)	The physical disk in the indicated slot is in use as a hot spare within a disk group.
Failed (status: down)	▪ Assigned	The physical disk in the indicated slot has been failed because of an unrecoverable error, an incorrect drive type or drive size, or by its operational state being set to failed.
	▪ Unassigned	
	▪ Hot Spare In Use	
	▪ Hot Spare Standby	
Replaced (status: up)	Assigned	The physical disk in the indicated slot has been replaced and is ready to be, or is actively being, configured into a disk group.
Pending Failure (status: down)	▪ Assigned	A SMART error has been detected on the physical disk in the indicated slot.
	▪ Unassigned	
	▪ Hot Spare In Use	
	▪ Hot Spare Standby	

"STATUS" CHANNEL	"MODE" CHANNEL	DESCRIPTION
None (status: warning)	None (status: warning)	The indicated slot is empty, or the array cannot detect the physical disk.
Undefined (status: down)		

✓ *Sensor* Dell PowerVault MDi Physical Disk ★★★★☆
 Ok

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Status Mode

Optimal Assigned

Channel ▾	ID ⇅	Last Value ⇅	Minimum ⇅	Maximum ⇅	
Downtime	-4				⚙
Mode	1	Assigned	Undefined	Assigned	⚙
Status	0	Optimal	Undefined	Optimal	⚙

Dell PowerVault MDi Physical Disk Sensor

Sensor in Other Languages

Dutch: **Dell PowerVault MDi Phy. Schijf**, French: **Disque physique Dell PowerVault MDi**, German: **Dell PowerVault MDi Phy. Datenträger**, Japanese: **Dell PowerVault MDi ? ? ? ? ? ?**, Portuguese: **Dell PowerVault MDi Disco Físico**, Russian: **Физ. диск Dell PowerVault MDi**, Simplified Chinese: **Dell PowerVault MDi ? ? ? ?**, Spanish: **Disco de Dell PowerVault MDi Phy.**

Remarks

- Works with Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i, and might support other models.
- [Requires](#) ⁶⁶⁹¹ Dell Modular Disk Storage Manager on the probe system. See the Knowledge Base: [Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?](#)

- Needs the IP address of the Storage Area Network (SAN) defined in the parent device settings.
 - This sensor supports devices with one drawer of hard-drives only. Multiple drawers are not supported and prevent sensor creation.
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
 - **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Dell Modular Disk Storage Manager

 This sensor requires the installation of the **Dell Modular Disk Storage Manager** program. You have to install it on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. For details about setup, please see **More** section below.

 Create this sensor on a device that has the SAN's IP address configured in the **IP Address/DNS Name** field of the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Physical Disks

Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Physical Disks	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📁 For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> 📘 This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Where do I find the Dell PowerVault Modular Disk Storage Manager for use with my MDi SAN?

- <https://kb.paessler.com/en/topic/38743>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

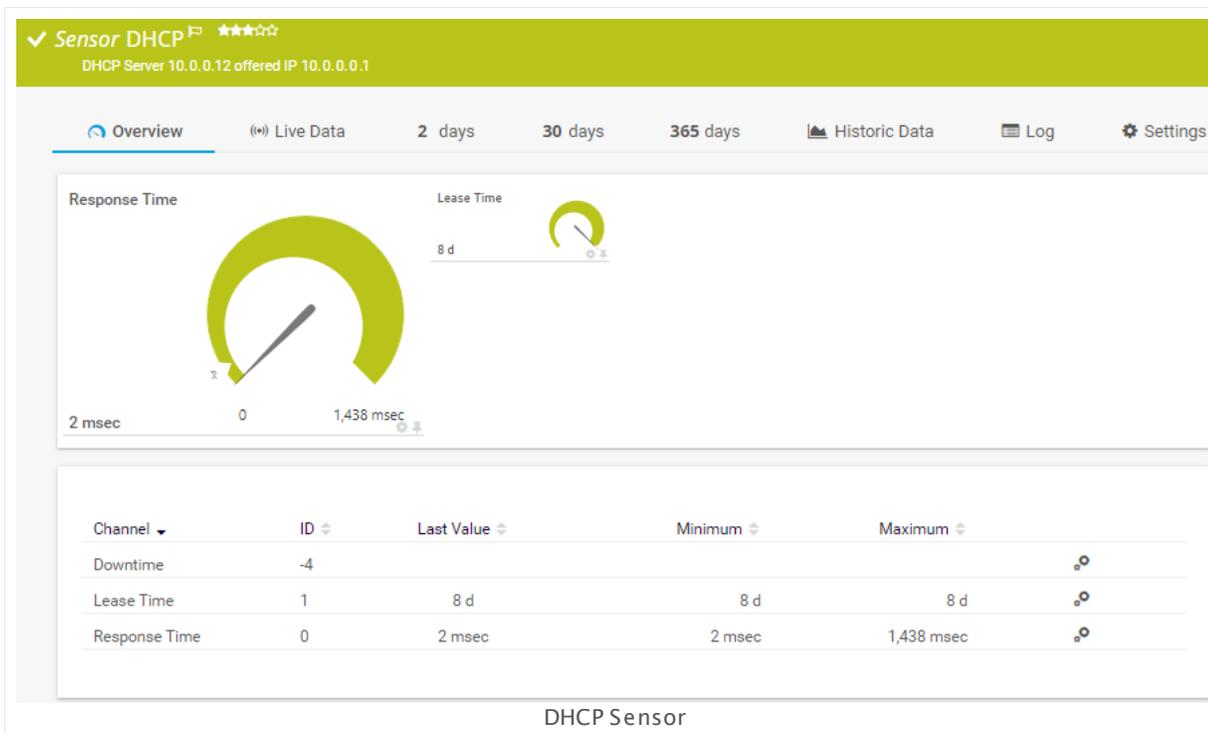
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.23 DHCP Sensor

The DHCP sensor monitors a Dynamic Host Configuration Protocol (DHCP) server. It sends a broadcast message to the network and waits for a DHCP server to respond. When creating this sensor, choose the network card on the probe system that will be used to send the broadcast message.

If a server responds, the sensor shows the following:

- Address of the server and the offered IP in the sensor message. You can check the server's response using [Regular Expressions](#).
- Response time (msec)
- Lease time given by the server (in days)



Remarks

- You can create this sensor only on a probe device (either local probe, a remote probe, or a cluster probe).
- The probe device where you create a DHCP sensor must have a static IP address. It cannot get its IP address from DHCP because this can cause a DHCP failure that will result in a severe issue for the probe device and you risk losing monitoring data.
- Do not use more than 2 DHCP sensors per device. Otherwise your DHCP sensors will show a timeout error.
- Knowledge Base: [How can I monitor a DHCP server in a specific network if there are several DHCP networks?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the desired network interfaces to monitor DHCP servers. PRTG will create one sensor for each network interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DHCP SPECIFIC

Specify Network Interface

Select the network adapters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) ^[181], as well as in [alarms](#) ^[219], [logs](#) ^[228], [notifications](#) ^[3216], [reports](#) ^[3262], [maps](#) ^[3276], [libraries](#) ^[3235], and [tickets](#) ^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DHCP SPECIFIC

MAC	Shows the MAC address of the network adapter that is used to send the broadcast message to the network. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Client IP	<p>Specify if you want to check the returned client IP with a regular expression. Choose between:</p> <ul style="list-style-type: none"> ▪ Don't check: The IP will only appear in the sensor message without further processes. ▪ Check: Enter the regular expression you want to use below.
Client IP Must Include	This field is only visible if you choose to Check the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP does not contain the defined string, the sensor shows a Down status .

DHCP SPECIFIC

For example, enter `10\0\5\.*` to make sure any answering DHCP server returns an client IP address starting with "10.0.5.". If it does not, the sensor will show an error. Leave empty to not use this field.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) 3704.

Client IP Must Not Include

This field is only visible if you choose to check the client IP above. In the response of the DHCP server, search using a regular expression. If the answer for the client IP **contains** the defined string, the sensor shows a **Down** status. See the example above. Leave empty to not use this field.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) 3704.

Server IP

Specify if you want to check the returned server IP with a regular expression. Choose between:

- **Don't check:** The IP will only appears in the sensor message without further processes.
- **Check:** Enter the regular expression you want to use below.

Server IP Must Include

This field is only visible if you choose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP **does not contain** the defined string, the sensor shows a **Down** status. See example above. Leave empty to not use this field.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) 3704.

Server IP Must Not Include

This field is only visible if you choose to check the server IP above. In the response of the DHCP server, search using a regular expression. If the answer for the server IP **contains** the defined string, the sensor shows a **Down** status. Leave empty to not use this field. See example above.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) 3704.

DHCP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
DHCP Server Change	<p>If there is more than one DHCP server in the network that may answer to the broadcast message, the sensor can receive an answer from a different DHCP server, compared to the last scan of the sensor. In this case, PRTG can write an entry to the system logs^[228]. Choose between:</p> <ul style="list-style-type: none"> ▪ Ignore: Do not write a log entry if the DHCP server changes. ▪ Write log entry: Write an entry to the system logs whenever the DHCP server changes between two sensor scans. <p> Regardless of this setting, those entries will always be added to the sensor log.</p>
Offered IP Change	<p>If the IP address offered by the DHCP server changes between two sensor scans, PRTG can write an entry to the system logs^[228]. Choose between:</p> <ul style="list-style-type: none"> ▪ Ignore: Do not write a log entry if the offered IP address changes. ▪ Write log entry: Write an entry to the system logs whenever the DHCP server offers a different IP address compared to the last sensor scan. <p> Regardless of this setting, those entries will always be added to the sensor log.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I monitor a DHCP server in a specific network if there are several DHCP networks?

- <https://kb.paessler.com/en/topic/64601>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
23 DHCP Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

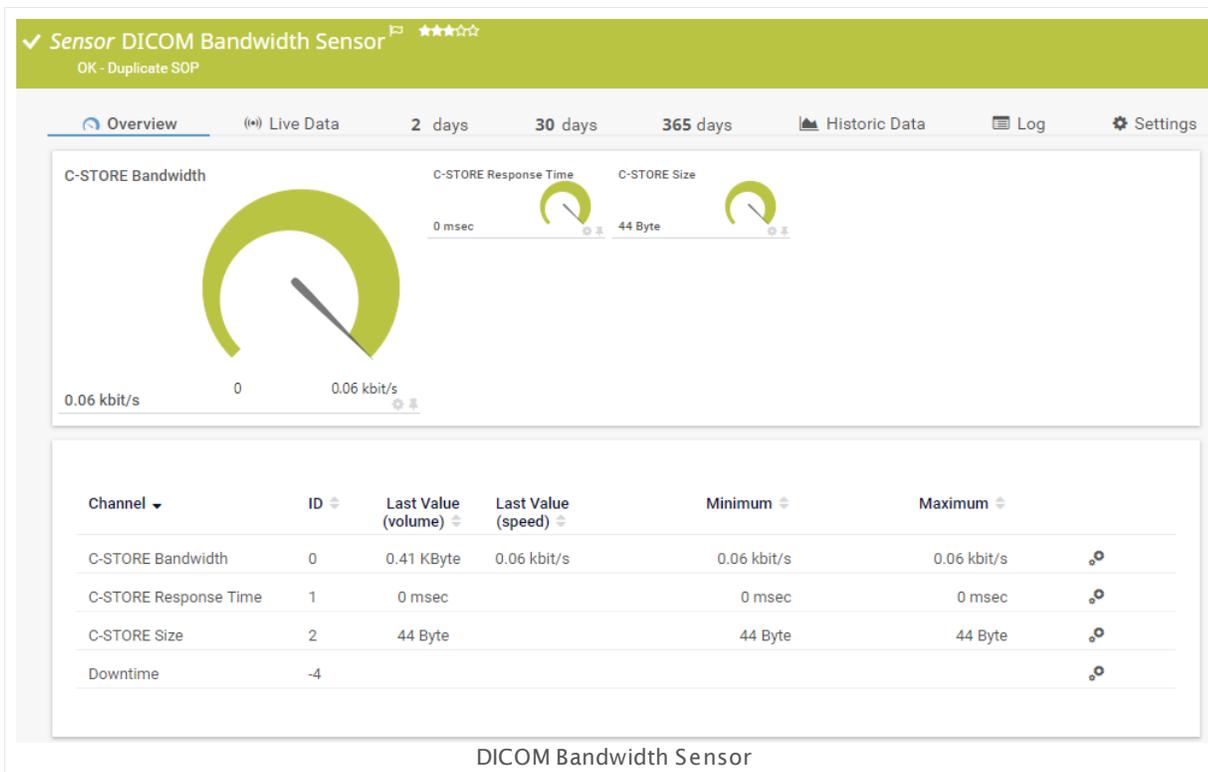
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.24 DICOM Bandwidth Sensor

The DICOM Bandwidth sensor monitors the bandwidth usage of a C-STORE request to a DICOM capable device. It sends one or more DICOM images and files that you have stored in a folder on a local disk or share and checks if the DICOM device can handle the C-STORE request. You can use the sensor to test your **Picture Archiving and Communication (PACS)** system, for example.

The sensor shows the following:

- C-STORE bandwidth (bandwidth usage of the sent files)
- Response time of the C-STORE request
- C-STORE size (total size of the sent files)



Sensor in Other Languages

Dutch: **DICOM Bandbreedte Sensor**, French: **Captteur de bande passante DICOM**, German: **DICOM-Bandbreiten-Sensor**, Japanese: **DI COM ? ? ? ? ? ?**, Portuguese: **Sensor de largura de banda do DICOM**, Russian: **Сенсор пропускной способности DICOM**, Simplified Chinese: **DICOM ? ? ? ? ?**, Spanish: **Sensor de anchura de banda de DICOM**

Remarks

- [Requires](#) ⁶⁹² .NET 4.6 or later on the probe system.

- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

- ✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#). If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.6 or .NET 4.7.

- 📖 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- 📘 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

DICOM CONNECTION

Calling Application Entity Title	<p>Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Called Application Entity Title	<p>Enter the configured Application Entity Title (AET) of the target system to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Port	<p>Enter the port of the DICOM interface that is used for the connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

BANDWIDTH SETTINGS

- File Path** Enter the full path to the folder where you have stored your DICOM files and images (ending with **.dcm**). The sensor will send all files in the folder to the target DICOM device with each request. You can use any folder on a disk or share that the PRTG probe on which the sensor runs has access to.
-  For example, enter **C:\DICOM** to send files that are stored in a folder named "DICOM" on the parent probe system.
 -  The path must contain ***.dcm** files. Enter the path without a backslash (\) at the end.

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[336] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
24 DICOM Bandwidth Sensor

Others

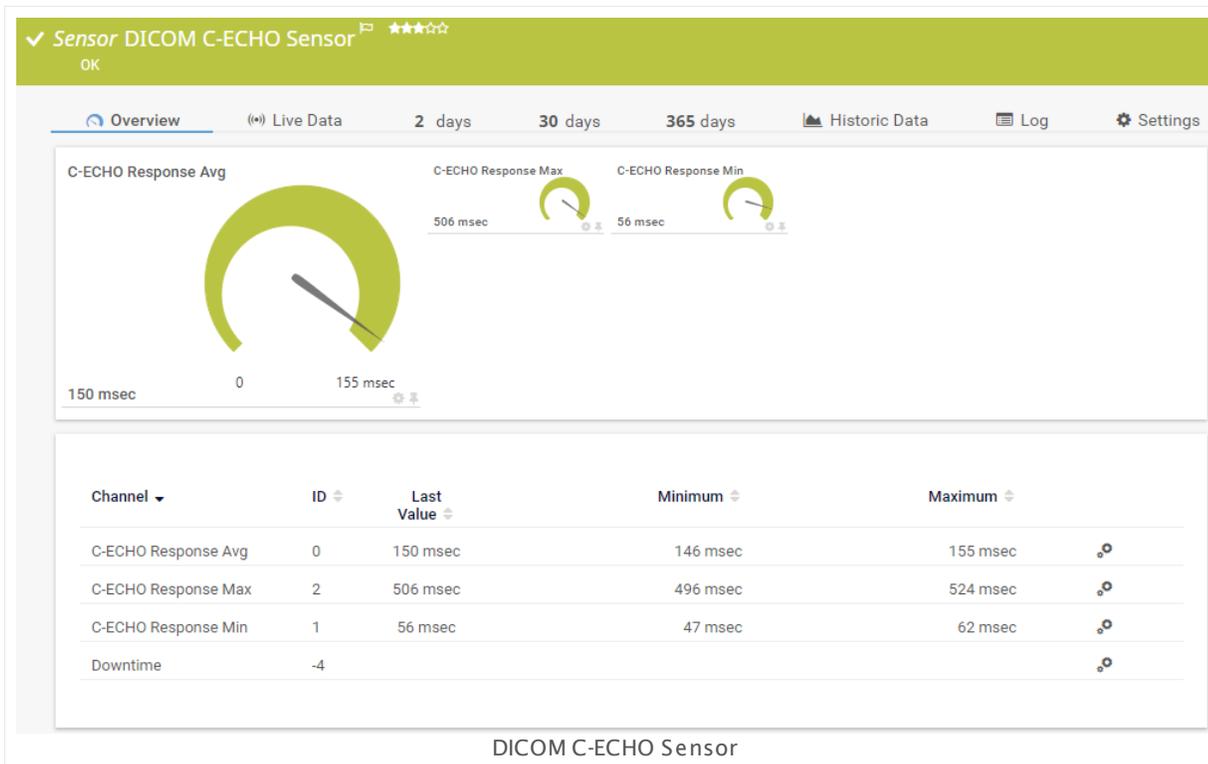
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.25 DICOM C-ECHO Sensor

The DICOM C-ECHO sensor monitors the availability of DICOM capable systems and devices by sending C-ECHO requests to the target system. C-ECHO is also known as DICOM-Ping. You can use the sensor to verify that the DICOM handshake is executed and that your target system is capable of answering DICOM messages.

The sensor shows the following:

- C-ECHO response time average, maximum, and minimum



Remarks

- [Requires](#) ⁷⁰¹ .NET 4.6 or later on the probe system.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

X This sensor type requires the [Microsoft .NET Framework](#) to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required [.NET](#) version (with latest update): .NET 4.6 or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DICOM CONNECTION

Calling Application Entity Title	<p>Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Called Application Entity Title	<p>Enter the configured Application Entity Title (AET) of the target system to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Port	<p>Enter the port of the DICOM interface that is used for the connection.</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

C-ECHO SETTINGS

C-ECHO Count	<p>Enter the number of C-ECHO requests that the sensor sends in a row for one interval. Please enter an integer value. The default value is 5.</p>
Ping Delay (ms)	<p>Enter the time in milliseconds the sensor will wait between two C-ECHO requests. Please enter an integer value. The default value is 10.</p>

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	--

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

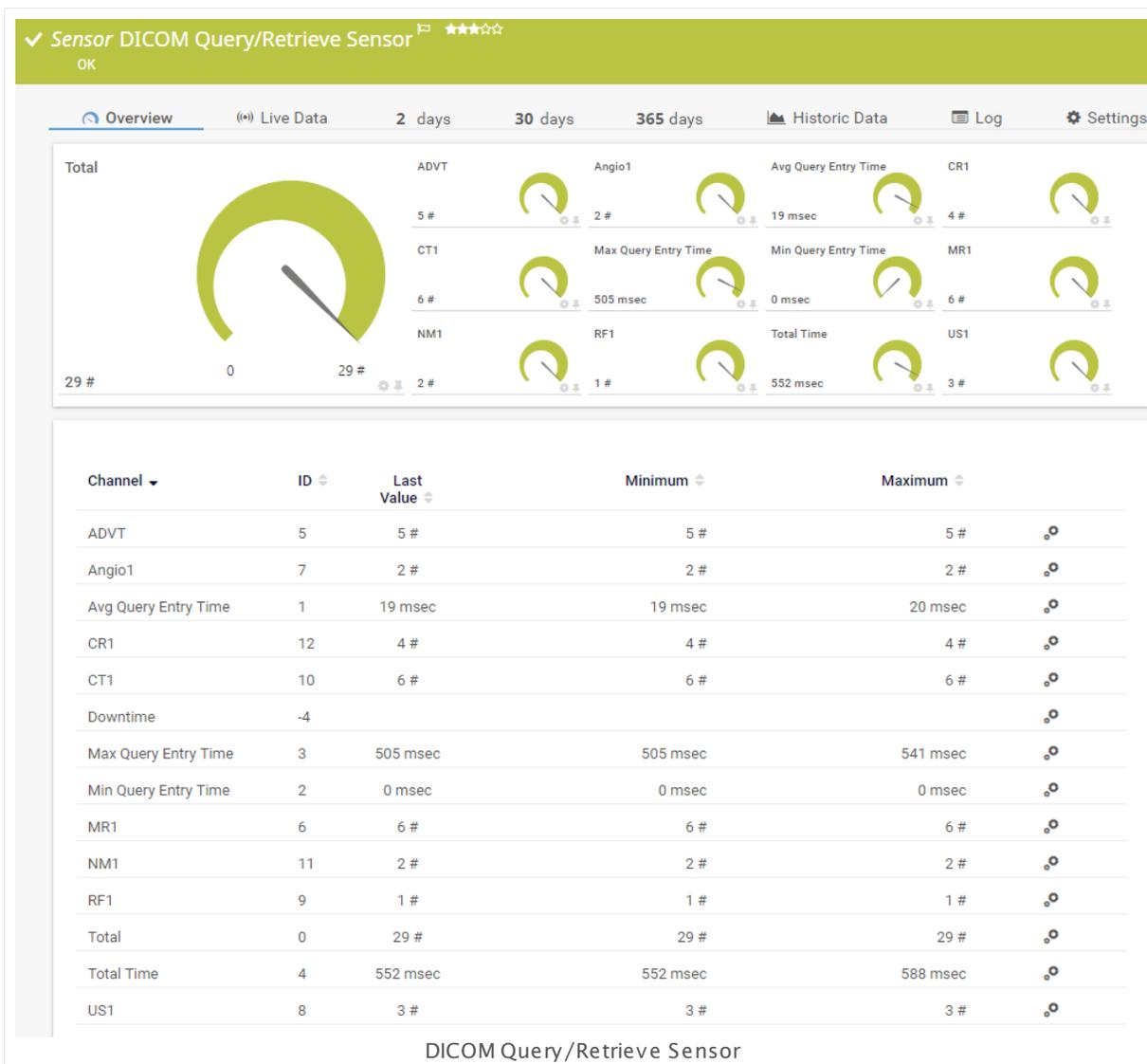
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.26 DICOM Query/Retrieve Sensor

The DICOM Query/Retrieve sensor monitors the C-FIND capability of DICOM capable systems and devices. It sends a C-FIND request or Modality Worklist (MWL) query to the target device and counts all found items. You can specify search levels to only count specific items.

The sensor shows the following:

- Minimum, maximum, and average time between receiving two responses
- Total communication time
- Total number of found items
- Number of found items by field



Sensor in Other Languages

Dutch: **DICOM Query/Retrieve Sensor**, French: **Capteur de requête/récupération de DICOM**, German: **DICOM-Abfrage-Sensor**, Japanese: **DI COM? ? ? /? ? ? ? ? ?**, Portuguese: **Sensor de recuperação/consulta do DICOM**, Russian: **Сенсор запроса/получения DICOM**, Simplified Chinese: **DICOM? ? /? ? ? ? ? ?**, Spanish: **Sensor de Consulta/Recuperación DICOM**

Remarks

- [Requires](#)^[711] .NET 4.6 or later on the probe system.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.6 or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DICOM CONNECTION

Calling Application Entity Title	<p>Enter the Application Entity Title (AET) of PRTG to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Called Application Entity Title	<p>Enter the configured Application Entity Title (AET) of the target system to initialize a DICOM connection.</p> <p> The AET is case sensitive and does not support special characters.</p>
Port	Enter the port of the DICOM interface that is used for the connection.

DICOM CONNECTION

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

QUERY/RETRIEVE SETTINGS

C-FIND Level Define the search level of the C-FIND request. Choose between:

- **Patient**: Retrieve data from the patient column via C-FIND. Enter a search key below.
- **Study**: Retrieve data from the study column via C-FIND. Enter a search key and modality below.
- **Series**: Retrieve data from the series column via C-FIND. Enter a search key and modality below.
- **Worklist**: Use a **Modality Worklist (MWL)** query to retrieve data from the worklist. Define desired fields below.

Search Key This field is not available for MWL queries. Enter a key to search for in the field that you selected above, for example, an instance UID, series UID, patient UID, or an asterisk (*) to search for all items.
Please enter a string.

Modality This field is only available if you search in the **Study** or **Series** column. Enter a modality in short form to search for, for example, **CT, MRI, US**, or an asterisk (*) to search for all modalities.
Please enter a string.

Filter Field This option is only available for MWL queries. Define a field of the worklist that you want to filter for. Choose between:

- **Station AET**
- **Station Name**
- **Modality**

Filter String This field is only available for MWL queries. Enter a string you want to filter for, for example, a station name, station AET, modality, or an asterisk (*) to filter for all items.

QUERY/RETRIEVE SETTINGS

Please enter a string.

Channel Field

This option is only available for MWL queries. Define which field you want to use to name the sensor channels. Choose between:

- **Station AET**
- **Station Name**
- **Modality**

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
26 DICOM Query/Retrieve Sensor

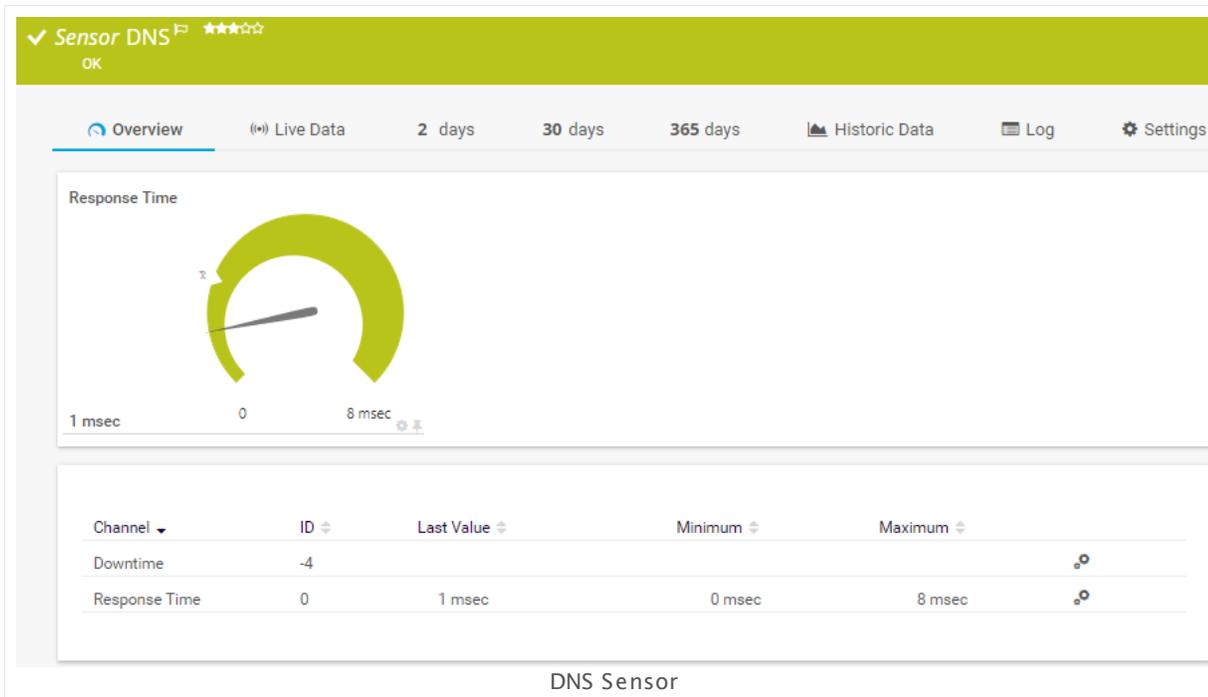
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.27 DNS Sensor

The DNS sensor monitors a Domain Name Service (DNS) server. It resolves a domain name and compares it to a given IP address.

- The sensor shows the response time of the DNS server.
- It will show a **Down status** ^[195] if the DNS server does not resolve a given domain name correctly.



Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DNS SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	<p>Enter the number of the port to which the sensor tries to connect. This must be the port the sensor's parent device is running the DNS service on. Usually you will use port 53. We recommend that you use the default value.</p> <p> The sensor connects to the IP Address or DNS Name value of the device^[402] on which you create it.</p>

DNS SPECIFIC

Domain	Enter the domain name that the sensor resolves using the Domain Name Service (DNS) server specified in the sensor's parent device settings ^[402] . You can enter an internet domain name here (for example, example.com) or a DNS name in your internal network (such as computer-xyz), depending on the type of DNS server you monitor. You can also enter an IP address here, but there might occur an error with certain query types.
Query Type	Select the type of query that the sensor sends to the DNS server. Choose between: <ul style="list-style-type: none">▪ Host address IPv4 (A)▪ Host address IPv6 (AAAA)▪ Authoritative name server (NS)▪ Start of a zone of authority marker (SOA)▪ Domain name pointer (PTR)▪ Mail exchange (MX)▪ Canonical name for an alias (CNAME)
Check Result	Define if the sensor checks the result from the DNS server. Choose between: <ul style="list-style-type: none">▪ Ignore result: Accept any valid answer of the DNS server.▪ Check result: Check if the response contains certain strings. Define below.
Value	<p>This field is only visible if you enable result checking above. Enter elements that the response of the DNS server must contain. Enter each entry in one line. The received result must contain at least one of the elements. If none of the element matches the response, the sensor will show a red Down status.</p> <p>For example, you can enter an IP address here if your Domain field contains a host name. Only if the host name is resolved to the correct IP address, your sensor will show a green Up status.</p>
Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.

DNS SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[338] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[310] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

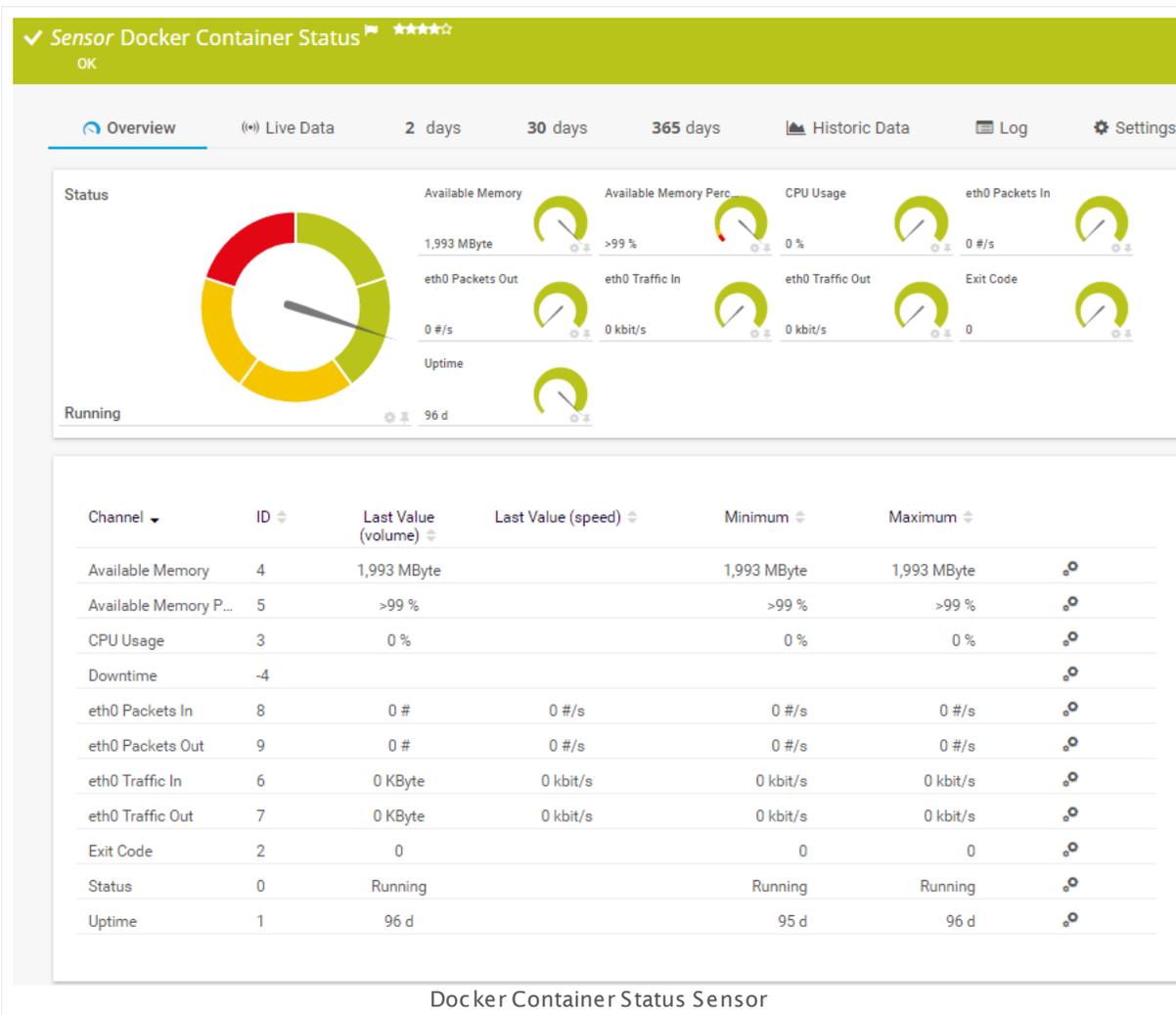
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.28 Docker Container Status Sensor

The Docker Container Status sensor monitors the status of a Docker container. It can show the following:

- Overall status of the container (create, running, paused, restarting, exited)
- Uptime
- Exit code
- CPU usage
- Available memory in bytes and percent



Sensor in Other Languages

Dutch: **Docker Container Status**, French: **État de conteneur Docker**, German: **Docker-Container-Zustand**, Japanese: **Dockerコンテナの状態**, Portuguese: **Status do Container Docker**, Russian: **Статус контейнера Docker**, Simplified Chinese: **Docker ? ? ? ?**, Spanish: **Estado de contenedor de Docker**

Remarks

- The parent device for this sensor must be the Docker machine on which the container runs that you want to monitor.
- You need to provide certificates and private keys to monitor Docker with this sensor. For details, see the Knowledge Base: [How can I create private key and certificate for the Docker sensor?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG requires an authentication with certificate and private key before you can actually add this sensor. Provide **Port** (usually **2375**), **Private Key**, and **Certificate** in the appearing dialog window and click **OK**. PRTG can now scan Docker for existing containers.

Select which Docker containers you want to monitor. PRTG creates one sensor for each container you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DOCKER SPECIFIC

Container	<p>Select the containers you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p>To better find what you want to monitor, especially in large tables, use the search function in the upper-right corner.</p>
-----------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DOCKER CREDENTIALS

Port	Enter the number of the port to which this sensor connects. The default port on which Docker over TLS runs is 2376 .
------	---

DOCKER CREDENTIALS

Private Key	<p>Provide the private key for the connection to Docker. If you have already created a key, you can use it here. Otherwise, please create a certificate on Docker first.</p> <p>Open the key with a text editor, copy everything that the file includes, and paste it here. Usually, the key starts with <code>-----BEGIN RSA PRIVATE KEY-----</code> and ends with <code>-----END RSA PRIVATE KEY-----</code></p> <p> See this Knowledge Base article on how to create a Docker certificate: How can I create private key and certificate for the Docker sensor?</p>
Certificate	<p>Provide the certificate for the connection to Docker. If you have already created a certificate, you can use it here. Otherwise, please create a certificate on Docker first.</p> <p>Open the certificate with a text editor, copy everything that the file includes, and paste it here. Usually, the certificate starts with <code>-----BEGIN CERTIFICATE-----</code> and ends with <code>-----END CERTIFICATE-----</code></p> <p> See this Knowledge Base article on how to create a Docker certificate: How can I create private key and certificate for the Docker sensor?</p>

DOCKER SPECIFIC

Container ID	Shows the ID of the container that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Container Name	Shows the name of the container that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Image	Shows the name of the image that was used to create the monitored Docker container. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Container Identification	Define how the sensor will identify the Docker container that it monitors. Choose between: <ul style="list-style-type: none">▪ By container ID (default): Use the ID of the Docker container to identify it.

DOCKER SPECIFIC

- **By container name:** Use the name of the Docker container to identify it. This is a good option if the IDs of your containers regularly change, for example, because of nightly deployments of your Docker containers.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I create private key and certificate for the Docker sensor?

- <https://kb.paessler.com/en/topic/67250>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

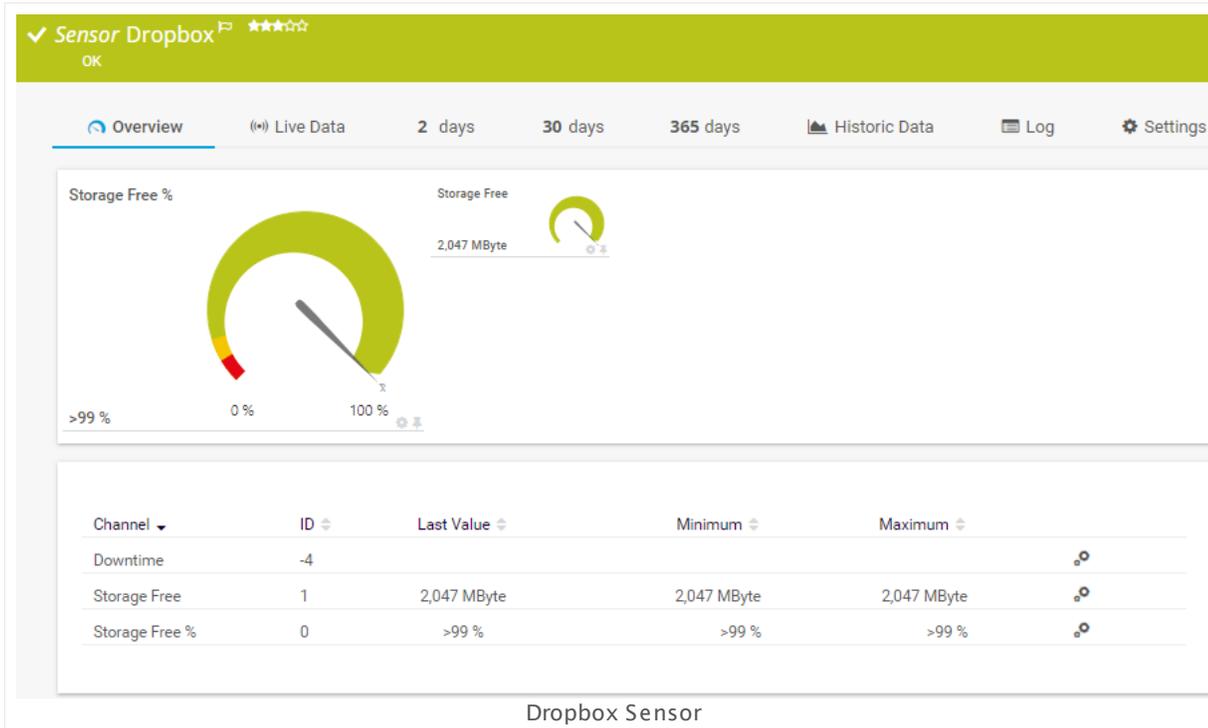
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.29 Dropbox Sensor

The Dropbox sensor monitors a Dropbox account using the Dropbox Application Programming Interface (API) and OAuth2. It shows the following:

- Free storage in bytes and percent



Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, see manual section [Authentication Using OAuth2](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DROPBOX CREDENTIALS

This sensor type uses OAuth2 authentication to get access to your Dropbox account.

 For details about the authentication approach, see section [Authentication Using OAuth2](#)⁷⁴⁹.

OAuth URL Click the button **Get Access Code** to connect this sensor to your Dropbox account using OAuth2. This is necessary to allow the sensor to query data from Dropbox. A new browser window appears.

Follow the steps in the window and confirm the permission for PRTG to connect to your Dropbox account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.

OAuth Code Paste the access code that you receive after completing the authorization process for PRTG at your Dropbox account. Click **OK** to define the [sensor settings](#)⁹³⁵.

 It is mandatory to connect this sensor to your Dropbox account to create this sensor. Complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)¹⁸¹, as well as in [alarms](#)²¹⁹, [logs](#)²²⁸, [notifications](#)³²¹⁶, [reports](#)³²⁵², [maps](#)³²⁷⁶, [libraries](#)³²³⁵, and [tickets](#)²³⁰.

Parent Tags Shows [Tags](#)¹³⁹ that this sensor [inherits](#)¹⁴⁰ from its [parent device, group, and probe](#)¹³³. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
- i** It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DROPBOX CREDENTIALS

- OAuth Code** Shows the authorization code that the sensor uses to get access to your Dropbox account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- i** You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Authentication Using OAuth2

 This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. Authorization Request

First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. Verifying Identity

This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.

 If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. Authorizing PRTG

Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. Getting Authorization Code

Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.

-  The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. Providing Authorization Code

Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. Requesting Access Token

After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access tokens are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. Retrieving Data

The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.30 Enterprise Virtual Array Sensor

The Enterprise Virtual Array sensor monitors an HP StorageWorks Enterprise Virtual Array (EVA) using the `ssu.exe` from [HP Command View EVA Software](#).

It can show the status of several HPE EVA modules, depending on the available measurement components:

- System controllers
- Enclosures
- Disks
- Disk groups
- Folders
- Hosts
- Snapshots
- Data replication
- Cabinets
- If the devices have measuring tools for fans and temperature, the sensor displays corresponding data as well.

For these EVA components, this sensor type can show the following:

- Operational status
- Predicted failures
- Accessible media
- Allocation in percent
- Availability for VRaids in bytes
- Exaggerated bytes
- Group host access
- Number of grouped and ungrouped disks
- Age of snapshots
- License status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Sensor in Other Languages

Dutch: **Enterprise Virtual Array**, French: **Enterprise Virtual Array**, German: **Enterprise Virtual Array**, Japanese: **Enterprise 仮想アレイ**, Portuguese: **Enterprise Virtual Array**, Russian: **Виртуальный массив предприятия**, Simplified Chinese: **??????**, Spanish: **Enterprise Virtual Array**

Remarks

- You have to explicitly specify the credentials of the EVA in the sensor settings.
 - [Requires](#)⁷⁵² the HP Command View EVA Software on the probe system, or the alternative described in this Knowledge Base article: [Do I really have to install the whole Command View on the probe to use the EVA sensor?](#)
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Command View

 The EVA sensor needs the HP Command View EVA Software to be installed on the probe system.

 If you do not want to install the whole command view tool, you can use another option. For details, see this Knowledge Base article: [Do I really have to install the whole Command View on the probe to use the EVA sensor?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

EVA CREDENTIALS

Scanning Mode

Specify the depth of the meta scan. Choose between:

- **Basic:** We recommend using this scanning mode. Various modules of your EVA will be available for monitoring.
- **Full Detail:** PRTG will scan for each disk of your EVA. Every disk will be listed in the module selection.

Select which modules you want to monitor. PRTG will create one sensor for each module you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

EVA SETTINGS

Modules Select the modules you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EVA CREDENTIALS

Username Enter the username for the EVA.

Password Enter the password for the EVA.

EVA SETTINGS

Module Shows the monitored module. You can adjust this setting if the module was renamed or moved to another folder. This way, PRTG can find the module again and the monitoring history will not be lost.

System Shows further information about the monitored module. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Module Type

Description

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.

EVA SETTINGS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Do I really have to install the whole Command View on the probe to use the EVA sensor?

- <https://kb.paessler.com/en/topic/55983>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

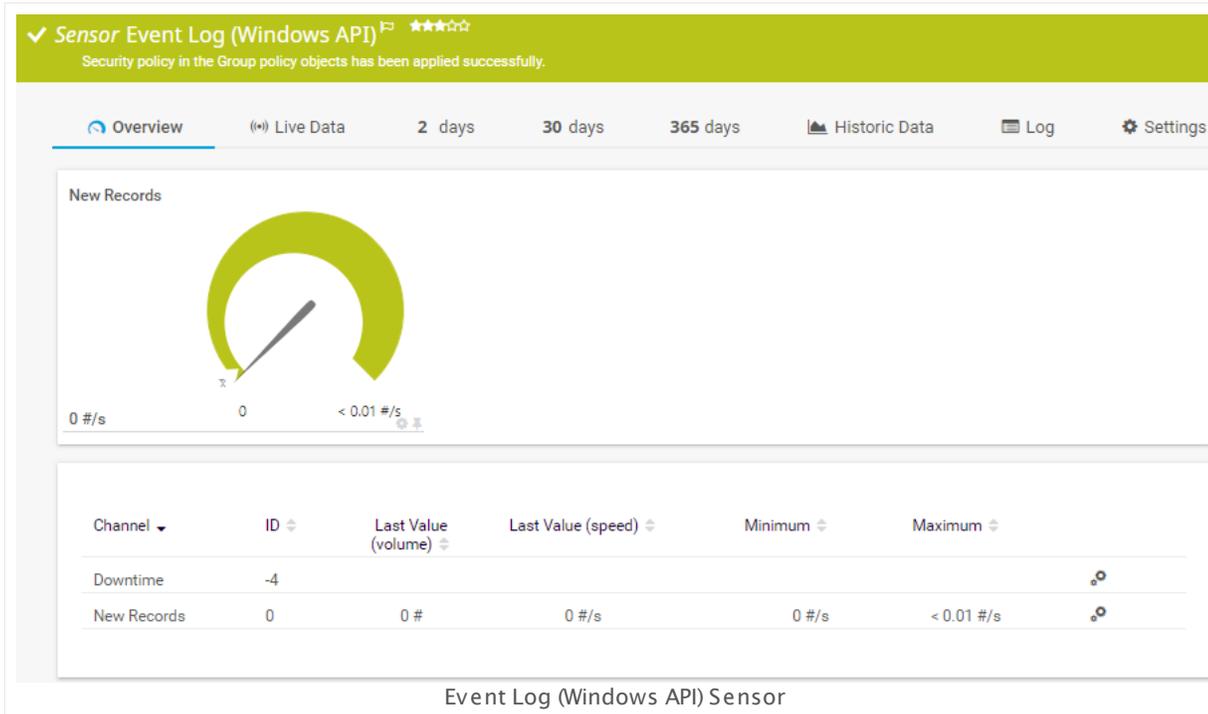
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.31 Event Log (Windows API) Sensor

The Event Log (Windows API) sensor monitors Event Log entries using Windows Application Programming Interface (API).

- It shows the number of new records per second (speed).



Sensor in Other Languages

Dutch: **Event Log (Windows API)**, French: **Log des événements (Windows API)**, German: **Ereignisprotokoll (Windows API)**, Japanese: **イベントログ (Windows API)**, Portuguese: **Log de Eventos do Windows (API)**, Russian: **Журнал событий (API Windows)**, Simplified Chinese: **???** (Windows API), Spanish: **Log de eventos (Windows API)**

Remarks

- Knowledge Base: [My Event Log sensor ignores changes in the event log. What can I do?](#)
- Knowledge Base: [How can I configure sensors using speed limits to keep the status for more than scanning interval?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS API EVENT LOG SPECIFIC

Log File	<p>Specify the log file that this sensor monitors. The Windows event log provides several different log files, which PRTG shows here. Choose between:</p> <ul style="list-style-type: none">▪ Application▪ System▪ Security▪ Directory Service▪ DNS Server▪ File Replication Service
----------	---

FILTER EVENT LOG ENTRIES

Event Type	<p>Specify the type of event that this sensor processes. Other event types cannot be processed. Choose between the following event types:</p> <ul style="list-style-type: none">▪ Any▪ Error▪ Warning▪ Information▪ Security Audit Success▪ Security Audit Failure
Filter by Source	<p>Filter all received events for a certain event source. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none">• Off: Do not filter by event source.• On: Enable filtering by event source.
Filter Type	<p>This field is only visible if you enable source filtering above. Choose between:</p> <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.

FILTER EVENT LOG ENTRIES

Match String (Event Source)	This field is only visible if you enable source filtering above. Enter an event source that you want to filter for. Depending on the kind of filter, the event source is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by ID	<p>Filter all received events for a certain event ID. If you enable this option, this sensor processes only messages that match the defined value(s). Choose between:</p> <ul style="list-style-type: none"> • Off: Do not filter by event ID. • On: Enable filtering by event ID.
Filter Type	<p>This field is only visible if you enable ID filtering above. Choose between:</p> <ul style="list-style-type: none"> • Include Filter: Include the specified value and disregard all other values. • Exclude Filter: Exclude the specified value and regard all other values.
Match Values (Event ID)	<p>This field is only visible if you enable ID filtering above. Enter an event ID that you want to filter for. Depending on the kind of filter, the event ID is processed (Include Filter) or not processed (Exclude Filter).</p> <p> The Event Log (Windows API) Sensor⁷⁶¹ supports more than one event ID. Using this sensor type, you can enter a comma-separated list of event IDs to filter for more than one ID.</p> <p> The WMI Event Log Sensor²⁸⁸⁹ supports filtering for only one ID.</p>
Filter by Category	<p>Filter all received events for a certain event category. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none"> • Off: Do not filter by event category. • On: Enable filtering by event category.
Filter Type	<p>This field is only visible if you enable category filtering above. Choose between:</p> <ul style="list-style-type: none"> • Include Filter: Include the specified value and disregard all other values. • Exclude Filter: Exclude the specified value and regard all other values.

FILTER EVENT LOG ENTRIES

Match String (Event Category)	This field is only visible if you enable category filtering above. Enter a category that you want to filter for. Depending on the kind of filter, the event category is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by User	Filter all received events for a certain event user. If you enable this option, this sensor only processes messages that match the defined value. Choose between: <ul style="list-style-type: none">• Off: Do not filter by event user.• On: Enable filtering by event user.
Filter Type	This field is only visible if you enable user filtering above. Choose between: <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event User)	This field is only visible if you enable user filtering above. Enter a username that you want to filter for. Depending on the kind of filter, the event user is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by Computer	Filter all received events for a certain event computer. If you enable this option, this sensor only processes messages that match the defined value. Choose between: <ul style="list-style-type: none">• Off: Do not filter by event computer.• On: Enable filtering by event computer.
Filter Type	This field is only visible if you enable computer filtering above. Choose between: <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event Computer)	This field is only visible if you enable computer filtering above. Enter a computer name that you want to filter for. Depending on the kind of filter, the event computer is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.

FILTER EVENT LOG ENTRIES

Filter by Message	<p>Filter all received events for a certain event message. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none">• Off: Do not filter by event message.• On: Enable filtering by event message.
Filter Type	<p>This field is only visible if you enable message filtering above. Choose between:</p> <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event Message)	<p>This field is only visible if you enable message filtering above. Enter a message that you want to filter for. Depending on the kind of filter, the event message is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.</p>

 The **Event Log (Windows API) Sensor** always performs a substring match. Please do not use any placeholder character. For example, enter **RAS** for any event source containing this string in partial or whole form.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?

- <https://kb.paessler.com/en/topic/59803>

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
31 Event Log (Windows API) Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

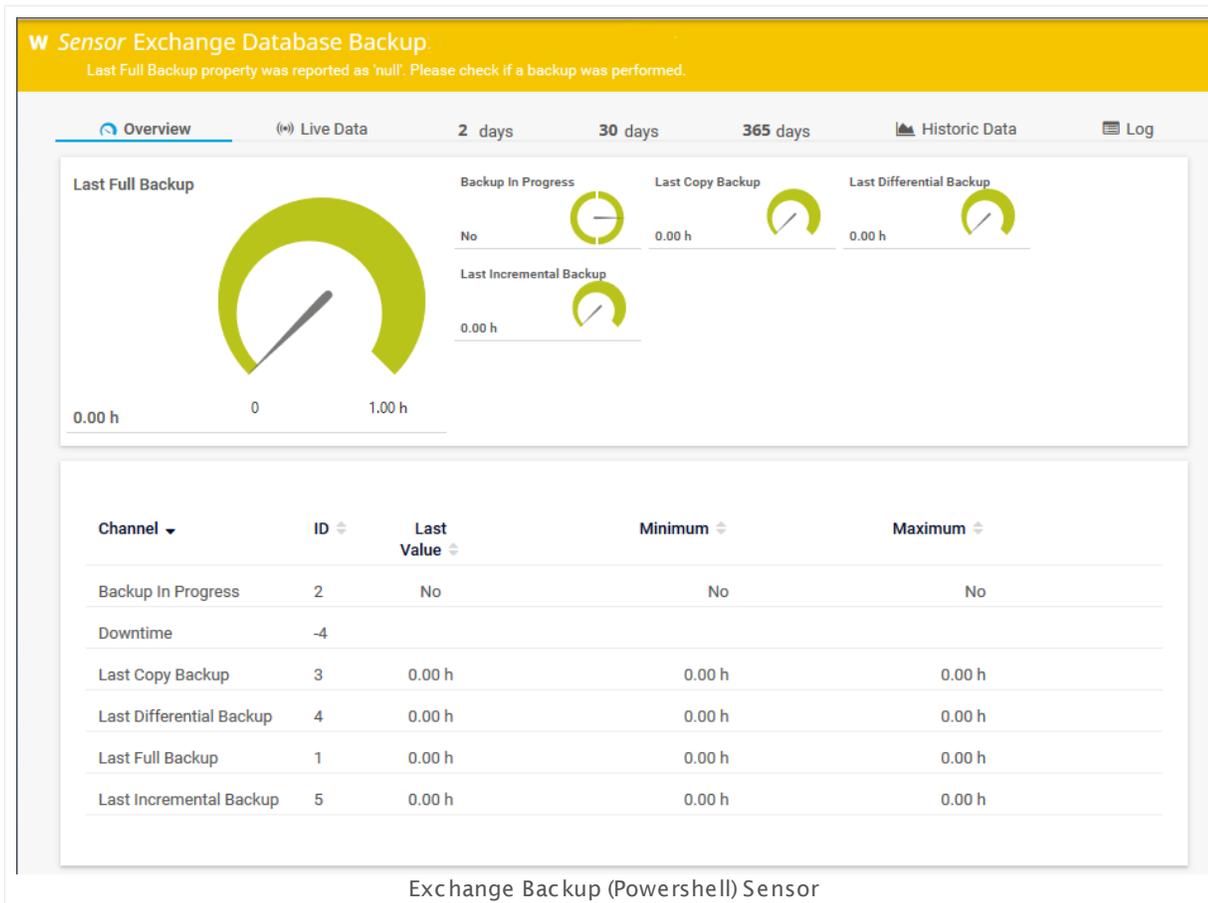
7.8.32 Exchange Backup (PowerShell) Sensor

The Exchange Backup (PowerShell) sensor monitors backups of an Exchange server using Remote PowerShell.

It can show several states of an Exchange database backup, for example:

- Passed time since the last full backup
- Passed time since the last copy backup
- Passed time since the last differential backup
- Passed time since the last incremental backup
- If a backup is currently running: Up [status](#)¹⁹⁵ for yes and no

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: Exchange Backup (PowerShell), French: Sauvegarde Exchange (PowerShell), German: Exchange Sicherung (PowerShell), Japanese: Exchange バックアップ (PowerShell),

Portuguese: **Exchange Backup (PowerShell)**, Russian: **Резервная копия Exchange (PowerShell)**, Simplified Chinese: Exchange? ? (PowerShell), Spanish: **Copia de seguridad de Exchange (PowerShell)**

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
 - Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - [Requires](#)^[774] Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
 - [Requires](#)^[774] the FQDN of the Exchange server in the [parent device settings](#)^[402].
 - [Requires](#)^[775] .NET 4.5 or higher on the probe system.
 - Knowledge Base: [PowerShell Sensors: FAQ](#)
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

-  This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.
-  In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.
-  For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

-  To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.
-  For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases	Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Database	Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result.

SENSOR SETTINGS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> 📘 This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
32 Exchange Backup (Powershell) Sensor

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

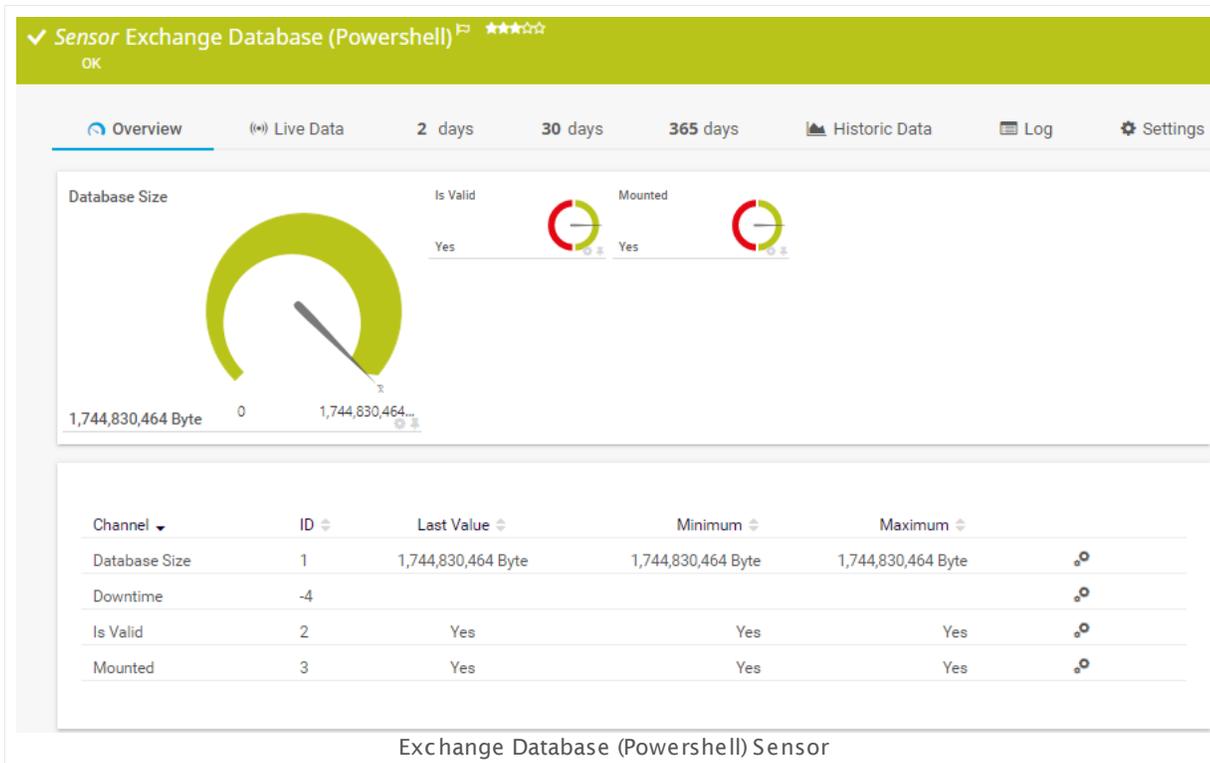
7.8.33 Exchange Database (PowerShell) Sensor

The Exchange Database (PowerShell) sensor monitors database information of an Exchange server using Remote PowerShell.

It shows several states of an Exchange database:

- Database size
- If the database is mounted
- If the database is recognized as valid

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: Exchange Database (PowerShell), French: Base de données Exchange (PowerShell), German: Exchange-Datenbank (PowerShell), Japanese: Exchange データベース (PowerShell), Portuguese: Exchange Banco de Dados (PowerShell), Russian: База данных Exchange (PowerShell), Simplified Chinese: Exchange ? ? ? (PowerShell), Spanish: Base de datos de Exchange (PowerShell)

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- [Requires](#)^[784] Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- [Requires](#)^[784] the FQDN of the Exchange server in the [parent device settings](#)^[402].
- [Requires](#)^[784] .NET 4.5 or later on the probe system.
- Knowledge Base: [PowerShell Sensors: FAQ](#)
- Knowledge Base: [How can I monitor additional values of Exchange databases?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

 This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

 In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.

 For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

 To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

 For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the **local system** (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SENSOR SETTINGS

Database	<p>Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
AutoRemount Database	<p>Define if you want the sensor to try to remount the database automatically if it is unmounted. Choose between:</p> <ul style="list-style-type: none"> ▪ Try to remount ▪ Just report the current reading and keep unmounted
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> ▪  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴.

SENSOR SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
-  Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
-  If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
-  If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: How can I monitor additional values of Exchange databases?

- <https://kb.paessler.com/en/topic/63229>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.34 Exchange Database DAG (Powershell) Sensor

The Exchange Database DAG (PowerShell) sensor monitors the Database Availability Group (DAG) status of a database on an Exchange server using Remote PowerShell.

It can show the following:

- Overall DAG status (for example, if it is mounted, failed, suspended)
- Copy status (active, not active)
- Content index status (healthy, crawling, error)
- If activation is suspended
- If log copy queue is increasing
- If replay queue is increasing
- Length of copy queue
- Length of Replay queue
- Number of single page restores

✓ Sensor Exchange Database DAG (Powershell) ★★★★☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Status



Healthy ⊗ ⊕

Activation Suspended		Active Copy		Content Index State		Copy Queue Length	
No	active	Healthy	0 #	Log Copy Queue Increa...		Log Replay Queue Incr...	
No	No	0 #	0 #	Replay Queue Length		Single Page Restore	
				0 #	0 #		

Channel	ID	Last Value	Minimum	Maximum	⊗ ⊕
Activation Suspended	2	No	No	No	⊗ ⊕
Active Copy	1	active	active	active	⊗ ⊕
Content Index State	8	Healthy	Healthy	Healthy	⊗ ⊕
Copy Queue Length	3	0 #	0 #	0 #	⊗ ⊕
Downtime	-4				⊗ ⊕
Log Copy Queue Increa...	4	No	No	No	⊗ ⊕
Log Replay Queue Increa...	5	No	No	No	⊗ ⊕
Replay Queue Length	6	0 #	0 #	1 #	⊗ ⊕
Single Page Restore	7	0 #	0 #	0 #	⊗ ⊕
Status	9	Healthy	Healthy	Healthy	⊗ ⊕

Exchange Database DAG (Powershell) Sensor

Sensor in Other Languages

Dutch: **Exchange Database DAG (PowerShell)**, French: **DAG de base de données Exchange (PowerShell)**, German: **Exchange-Datenbank DAG (PowerShell)**, Japanese: **Exchange データベース DAG (PowerShell)**, Portuguese: **Exchange Banco de Dados DAG (PowerShell)**, Russian: **ДAG базы данных Exchange (PowerShell)**, Simplified Chinese: **Exchange ? ? ? DAG (PowerShell)**, Spanish: **Base de datos DAG de Exchange (PowerShell)**

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
 - Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - [Requires](#)⁷⁹⁵ Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
 - [Requires](#)⁷⁹⁶ the FQDN of the Exchange server in the [parent device settings](#)⁴⁰².
 - [Requires](#)⁷⁹⁶ .NET 4.5 or later on the probe system.
 - Make sure that the Exchange database is mounted on the target device. Otherwise, you might not be able to properly add the sensor.
 - Knowledge Base: [PowerShell Sensors: FAQ](#)
 - Knowledge Base: [How can I monitor additional values of Exchange databases?](#)
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

-  This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.
-  In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.
-  For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

-  To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.
-  For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

-  This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

-  For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server databases you want to monitor. PRTG creates one sensor for each database you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Exchange Databases	Select the databases you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Database	Shows the name of the monitored database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	Define what PRTG will do with the sensor results. Choose between:

SENSOR SETTINGS

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: How can I monitor additional values of Exchange databases?

- <https://kb.paessler.com/en/topic/63229>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

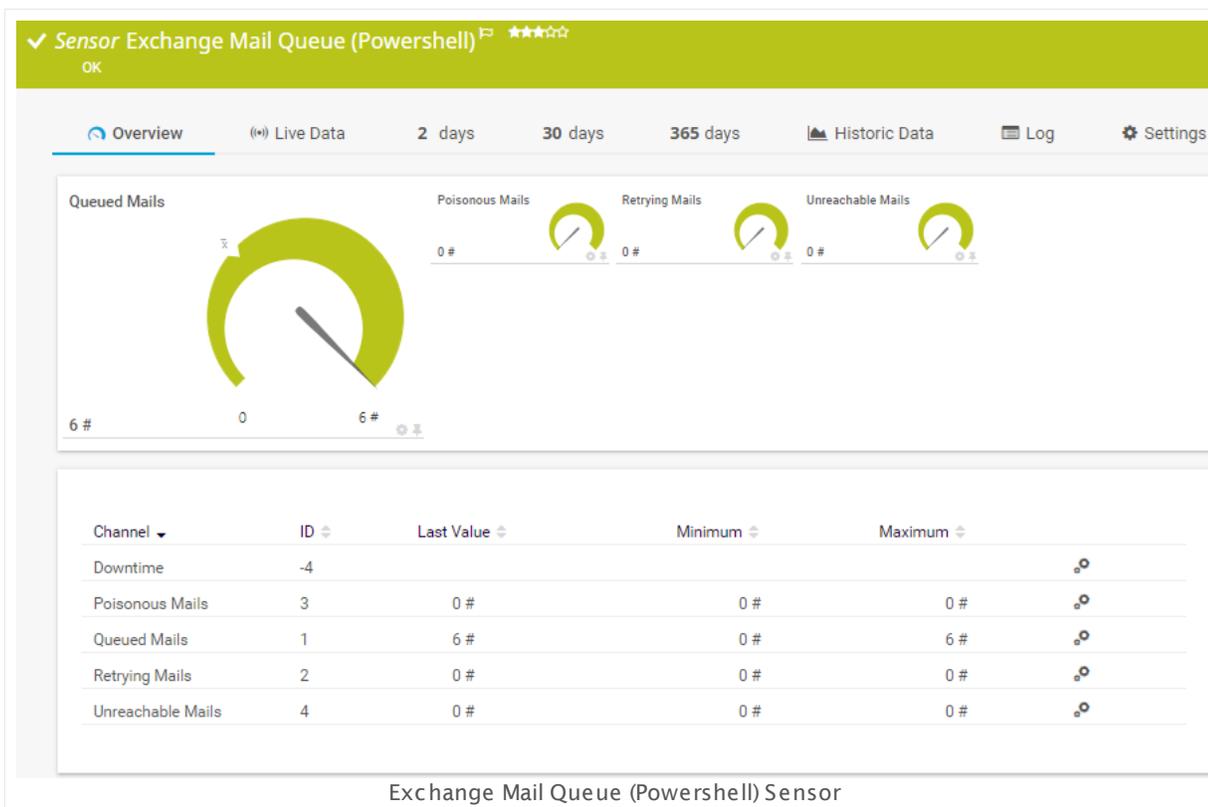
7.8.35 Exchange Mail Queue (PowerShell) Sensor

The Exchange Mail Queue (PowerShell) sensor monitors the number of items in the outgoing mail queue of an Exchange server using Remote PowerShell.

It can show the following:

- Number of queued mails
- Number of retrying mails
- Number of unreachable mails
- Number of poisonous mails

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Exchange Mail Wachtrij (PowerShell)**, French: **File d'attente de messagerie Exchange (PowerShell)**, German: **Exchange Nachrichtenwarteschlange (PowerShell)**, Japanese: **Exchange Mail キュー (PowerShell)**, Portuguese: **Exchange Fila de Email (PowerShell)**, Russian: **Очередь почтовых сообщений Exchange (PowerShell)**, Simplified Chinese: **Exchange ? ? ? ? (PowerShell)**, Spanish: **Cola de correo de Exchange (PowerShell)**

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- [Requires](#) ⁸⁰⁵ Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- [Requires](#) ⁸⁰⁵ the FQDN of the Exchange server in the [parent device settings](#) ⁴⁰².
- [Requires](#) ⁸⁰⁵ .NET 4.5 or later on the probe system.
- Knowledge Base: [PowerShell Sensors: FAQ](#)
- Knowledge Base: [What types of Exchange transport queues are there?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

 This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

 In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.

 For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

 To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

 For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the roles you want to monitor. PRTG creates one sensor for each role you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Hub-Transport or Edge-Server Select the roles you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage.  This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.
---------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: What types of Exchange transport queues are there?

- <https://kb.paessler.com/en/topic/55413>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

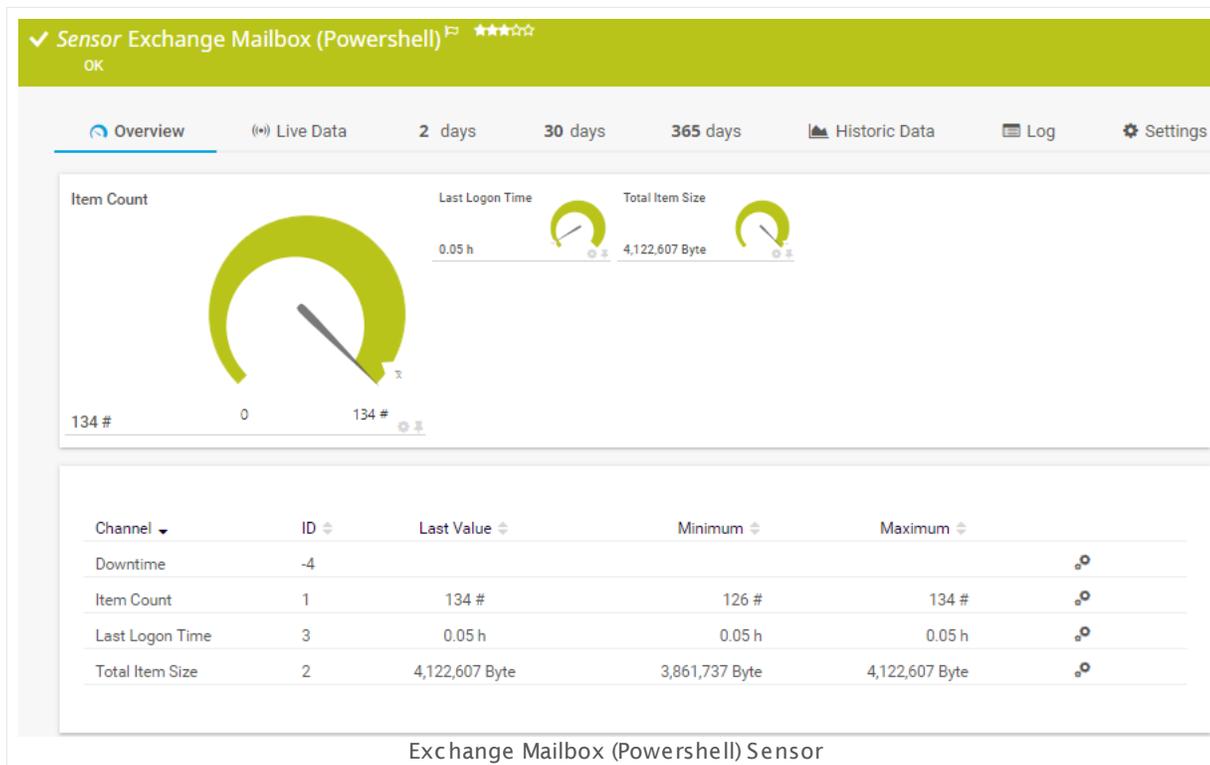
7.8.36 Exchange Mailbox (Powershell) Sensor

The Exchange Mailbox (PowerShell) sensor monitors mailboxes of an Exchange server using Remote PowerShell.

It shows several states of a mailbox, for example:

- Total size of items in place
- Number of items in place
- Passed time since the last mailbox logon

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Exchange Postbus (PowerShell)**, French: **Boîte aux lettres Exchange (PowerShell)**, German: **Exchange Postfach (PowerShell)**, Japanese: **Exchange Mailbox (PowerShell)**, Portuguese: **Exchange Caixa de Email (PowerShell)**, Russian: **Почтовый ящик Exchange (PowerShell)**, Simplified Chinese: **Exchange ? ? (PowerShell)**, Spanish: **Buzón de Exchange (PowerShell)**

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- [Requires](#)^[815] Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- [Requires](#)^[815] the FQDN of the Exchange server in the [parent device settings](#)^[402].
- Requires elevated rights for the user of this sensor on the Exchange system. It is not sufficient to have administrator rights. For details, see the Knowledge Base: [I have problems with the PowerShell Exchange sensors, what can I do?](#) (solution (2) in the reply)
- [Requires](#)^[815] .NET 4.5 or later on the probe system.
- Knowledge Base: [PowerShell Sensors: FAQ](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

 This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

 In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.

 For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

 To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

 For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server mailboxes you want to monitor. PRTG creates one sensor for each mailbox you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Mailboxes Select the mailboxes you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

- Mailbox Name** Shows the name of the monitored mailbox. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result**: Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

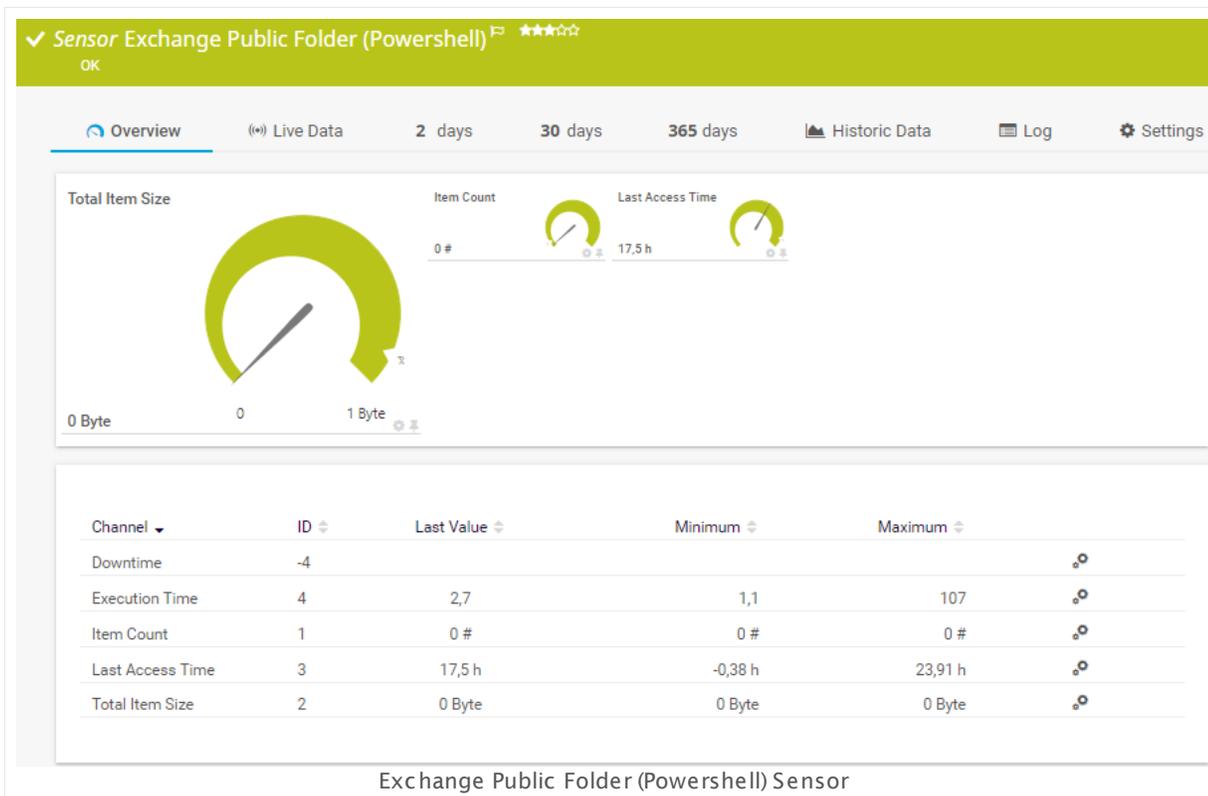
7.8.37 Exchange Public Folder (PowerShell) Sensor

The Exchange Public Folder (PowerShell) sensor monitors public folders and subfolders of an Exchange server using Remote PowerShell.

It can show several states of a public folder:

- Total size of items in place
- Number of items in place
- Passed time since the last access

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Exchange Openbare Map (PowerShell)**, French: **Dossier public Exchange (PowerShell)**, German: **Exchange Öffentlicher Ordner (PowerShell)**, Japanese: **Exchange パブリックフォルダー (PowerShell)**, Portuguese: **Exchange Pasta Pública (PowerShell)**, Russian: **Общая папка Exchange (PowerShell)**, Simplified Chinese: **Exchange ? ? ? ? (PowerShell)**, Spanish: **Carpeta pública de Exchange (PowerShell)**

Remarks

- The parent device for this sensor must be the Exchange server (version 2010 or higher) that hosts the database you want to monitor.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- [Requires](#)^[825] Remote PowerShell and Remote Exchange Management Shell on the target servers and PowerShell 2.0 on the probe system.
- [Requires](#)^[825] the FQDN of the Exchange server in the [parent device settings](#)^[402].
- [Requires](#)^[825] .NET 4.5 or later on the probe system.
- Knowledge Base: [PowerShell Sensors: FAQ](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell and Remote Exchange Management Shell

 This sensor type uses PowerShell commands. To monitor Exchange servers with this sensor, you have to enable **Remote PowerShell** and **Remote Exchange Management Shell** on the target servers that you want to monitor. Also ensure you have installed **PowerShell 2.0** or later on your probe machine.

 In larger environments, the default memory limit for the remote shell might be insufficient. This might result in the error message **The WSMAN provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell.

 For more information, please see this Knowledge Base article: [How do I enable and use remote commands in Windows PowerShell?](#)

Requirement: Fully Qualified Domain Name (FQDN)

 To connect to Exchange servers, this sensor type needs the **fully qualified domain name (FQDN)**. In PRTG's device settings of the Exchange server, provide the FQDN instead of the IP address.

 For more information, see this Knowledge Base article: [I have problems with the PowerShell Exchange sensors, what can I do?](#)

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Exchange server mailboxes you want to monitor. PRTG creates one sensor for each mailbox you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Public Folder	Select the folders you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
---------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
-------------	--

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Public Folder	Shows the name of the monitored folder. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage.

SENSOR SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Resolving Exchange PowerShell Sensors Issues

- <https://kb.paessler.com/en/topic/54353>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

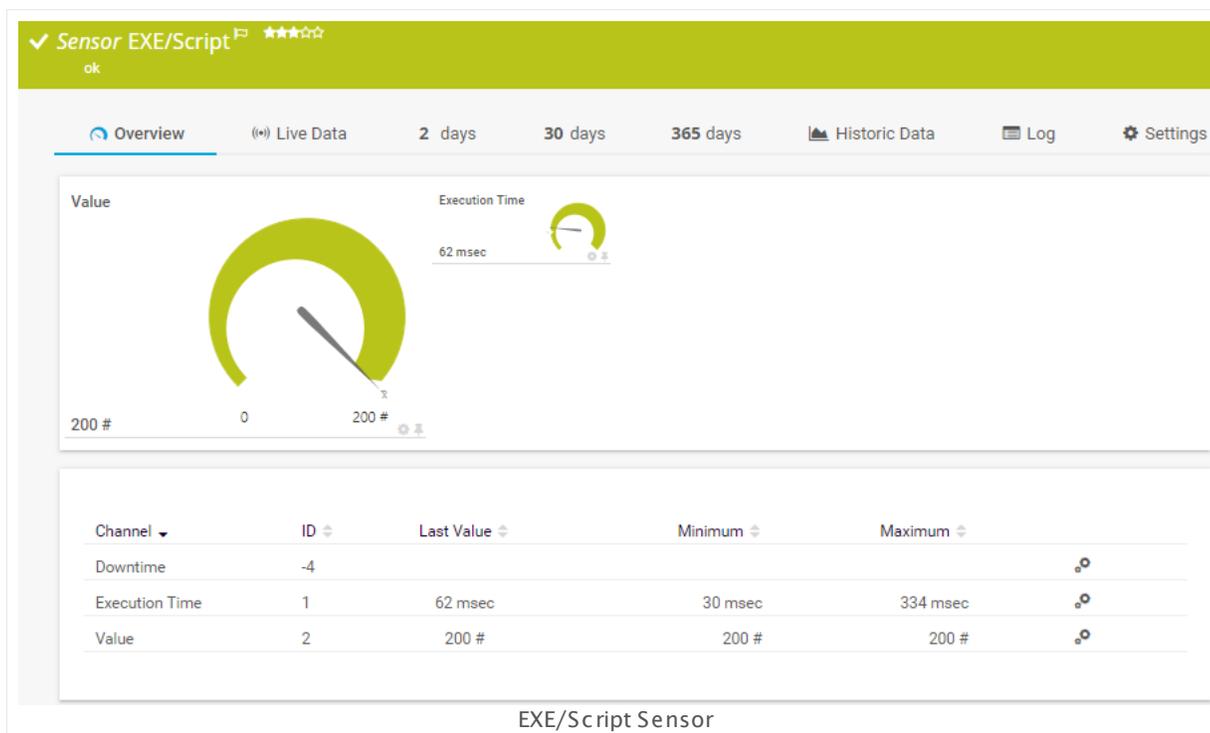
7.8.38 EXE/Script Sensor

The EXE/Script sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, PowerShell) on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API).

This sensor can show the following:

- One value returned by the executable file or script (in one channel only)
- Execution time

For details about the return value format, see section [Custom Sensors](#).



Sensor in Other Languages

Dutch: **EXE/Script**, French: **Script/EXE**, German: **Programm/Skript**, Japanese: **EXE / スクリプト**, Portuguese: **EXE/Script**, Russian: **EXE/скрипт**, Simplified Chinese: **EXE/? ?**, Spanish: **EXE/Script**

Remarks

- The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the [WMI Custom Sensor](#).

- Knowledge Base: [What is the Mutex Name in PRTG's EXE/Script Sensor's settings?](#)
- Knowledge Base: [How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?](#)
- Knowledge Base: [How can I show special characters with EXE/Script sensors?](#)
- Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)  add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script	<p>Select an executable file from the list. The sensor will execute it with every scanning interval.</p> <p>In this list, files in the corresponding \Custom Sensors\EXE sub-directory of the probe system's PRTG program directory are shown (see Data Storage³⁷³⁴). To appear in this list, store the file into this folder ending in BAT, CMD, DLL, EXE, PS1, or VBS.</p> <p>To show the expected sensor values and status, your files must use the correct format for the returned values (in this case, value:message to standard output). The exit code of the file determines the sensor status¹⁹⁵.</p> <p> For detailed information on how to build custom sensors and for the expected return format, see section Custom Sensors³⁶³⁹ for more information.</p> <p> When using custom sensors on the Cluster Probe, please copy your files to every cluster node installation.</p>
Value Type	<p>Define what kind of values your executable or script file gives back. Choose between:</p> <ul style="list-style-type: none">▪ Integer: An integer is expected as return value. If the script gives back a float, PRTG will display the value 0.▪ Float: A float is expected as return value, with a dot (.) between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they produce a buffer overflow.▪ Counter: Your script returns an integer that increases. PRTG will show the difference between the values of two sensor scans.  A counter must return an integer, float is not supported. <p> The sensor cannot handle string values.</p>
Channel Name	<p>Enter a name for the channel in which the sensor shows returned values. Please enter a string. This is for display purposes only. You can change the name later in the sensor's channel settings³¹⁶⁰.</p>
Unit String	<p>Enter the unit for the values that this sensor returns. Please enter a string. This unit string is used for display purposes and will be shown in graphs, data tables, and gauges. If you want to change the Unit after having created the sensor, you can change it in the sensor's channel settings³¹⁶⁰.</p>

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

EXE/Script	Shows the executable or script file that the sensor executes with each sensor scan as defined on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	<p>If your executable or script file catches command line parameters, you can define them here. You can use placeholders as well.</p> <p> For a full list of all placeholders, see section Custom Sensors³⁶⁵⁴.</p> <p>Please enter a string or leave the field empty.</p> <p> You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section Escape Special Characters and Whitespaces in Parameters⁸⁴⁵ for details.</p>
Environment	<p>Choose if PRTG command line parameters will also be available as environment parameters.</p> <ul style="list-style-type: none"> ▪ Default Environment: Do not provide PRTG placeholders' values in the environment. Choose this secure option if you are not sure. ▪ Set placeholders as environment values: From within your executable or script, the values of PRTG's command line parameters will be available via environment variables. For example, you can then read and use the current host value of the PRTG device this EXE/script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables. <p> For a full list of all available variables, see section Custom Sensors³⁶⁵⁶ for more information.</p>
Security Context	<p>Define the Windows user account that the sensor uses to run the executable or script file. Choose between:</p> <ul style="list-style-type: none"> ▪ Use security context of probe service: Run the selected file under the same Windows user account the probe runs on. By default, this is the Windows system user account (if not manually changed). ▪ Use Windows credentials of parent device: Use the Windows user account defined in the settings of the parent device this sensor is created on. Please open the parent device settings⁴⁰² of this sensor to change these Windows credentials.

SENSOR SETTINGS

Mutex Name	<p>Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously).</p> <p>This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.</p> <p> For more information, see this Knowledge Base article: What is the Mutex Name in the PRTG EXE/Script Sensor settings?</p>
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>
Value Type	<p>Shows the expected value type that you chose on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p> <p> The sensor cannot handle string values.</p>
If Value Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none">▪ Ignore changes (default): The sensor takes no action on change.▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>3170</small> whenever the sensor value changes.
EXE Result	<p>Define what this sensor will do with the result that the executable file gives back. Choose between:</p> <ul style="list-style-type: none">▪ Discard EXE result: Do not store the script result.▪ Write EXE result to disk: Store the last result received from the script to the Logs (Sensors) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval. <p> For information on how to find the folder used for storage, see section Data Storage <small>3734</small>.</p>

SENSOR SETTINGS

- **Write EXE result to disk in case of error:** Store the last result received from the script only if the sensor is in a down status. File name: **Result of Sensor [ID].txt**, located in the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). Enable this option if you do not want failures to be overwritten by a following success of the script.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Escape Special Characters and Whitespaces in Parameters

X You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings.

A We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#)³⁶⁵⁰ for details.

More

Information about custom scripts and executables

- [Custom Sensors](#)³⁶³⁷
- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵

Knowledge Base: What is the Mutex Name in the PRTG EXE/Script Sensor settings?

- <https://kb.paessler.com/en/topic/6673>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.39 EXE/Script Advanced Sensor

The EXE/Script Advanced sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, PowerShell) on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API). The return value of this sensor must be valid XML or JSON.

- The sensor can show values returned by the executable file or script in multiple channels.

For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.



Channel	ID	Last Value	Minimum	Maximum
Demo Custom	5	855 Pieces	855 Pieces	855 Pieces
Demo Disk Free	3	38.4487 %	38.4487 %	38.4487 %
Demo Minimum Example	2	3 #	3 #	3 #
Demo Network Speed	4	996 Mbit/s	996 Mbit/s	996 Mbit/s
Downtime	-4			

EXE/Script Advanced Sensor

Sensor in Other Languages

Dutch: **EXE/Script Geavanceerd**, French: **Script/EXE version améliorée**, German: **Programm/Skript (Erweitert)**, Japanese: **EXE / スクリプト(アドバンスト)**, Portuguese: **EXE/Script avançado**, Russian: **Расширенный сенсор EXE/скрипта**, Simplified Chinese: **?? EXE/? ?**, Spanish: **EXE/Script Avanzado**

Remarks

- This sensor [does not support more than 50 channels](#)⁸⁴⁸ officially.
- The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

- If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the [WMI Custom Sensor](#)²⁸⁶⁷.
- Knowledge Base: [What is the Mutex Name in PRTG's EXE/Script Sensor's settings?](#)
- Knowledge Base: [How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?](#)
- Knowledge Base: [How can I show special characters with EXE/Script sensors?](#)
- Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
- Knowledge Base: [How can I use meta-scans for custom EXE/Script sensors?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

EXE/Script

Select an executable file from the list. The sensor will execute it with every scanning interval.

This list shows all files available in the corresponding **\Custom Sensors\EXEXML** sub-directory of the probe system's PRTG program directory (see [Data Storage](#)³⁷³⁴). To appear in this list, please store the files into this folder ending in BAT, CMD, DLL, EXE, PS1, or VBS.

To show the expected values and sensor status, your files must return the expected XML or JSON format to standard output. Values and message must be embedded in the XML or JSON.

SENSOR SETTINGS

-  For detailed information on how to build custom sensors and for the expected return format, see section [Custom Sensors](#) for more information.
-  When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

-  Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

- | | |
|-------------|---|
| Sensor Name | Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets . |
| Parent Tags | Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here. |
| Tags | <p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none">  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>). |

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

EXE/Script Shows the executable or script file that the sensor executes with each scan as defined on sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Parameters If your executable or script file catches command line parameters, you can define them here. You can use placeholders as well.

 For a full list of all placeholders, see the API documentation in your PRTG installation. See section [Custom Sensors](#)³⁶⁵⁴ for more information.

Please enter a string or leave the field empty.

 You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section [Escape Special Characters and Whitespaces in Parameters](#)⁸⁵⁷¹ for details.

Environment Choose if PRTG command line parameters will also be available as environment parameters.

- **Default Environment:** Do not provide PRTG placeholders' values in the environment. Choose this secure option if you are not sure.
- **Set placeholders as environment values:** From within your executable or script, the values of PRTG command line parameters will be available via environment variables. For example, you can then read and use the current **host** value of the PRTG device this EXE/Script sensor is created on from within your script. This option can mean a security risk, because also credentials are provided in several variables.

 For a full list of all available variables, see section [Custom Sensors](#)³⁶⁵⁶.

Security Context Define the Windows user account that the sensor uses to run the executable or script file. Choose between:

SENSOR SETTINGS

- **Use security context of probe service:** Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed).
- **Use Windows credentials of parent device:** Use the Windows user account defined in the settings of the parent device this sensor is created on. Please open the [parent device settings](#)⁴⁰² of this sensor to change these Windows credentials.

Mutex Name

Define any desired mutex name for the process. All EXE/Script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.

 For more information, see this Knowledge Base article: <http://kb.paessler.com/en/topic/6673>

Timeout (Sec.)

Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

EXE Result

Define what the sensor will do with the results the executable file gives back. Choose between:

- **Discard EXE result:** Do not store the script result.
- **Write EXE result to disk:** Store the last result received from the script to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: **Result of Sensor [ID].txt**. This is for debugging purposes. The file will be overridden with each scanning interval.

 For information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

- **Write EXE result to disk in case of error:** Store the last result received from the script only if the sensor is in a down status. File name: **Result of Sensor [ID].txt**, located in the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). Enable this option if you do not want failures to be overwritten by a following success of the script.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

 The **Stack Unit** option for stacking graphs will only work if you explicitly define the same **<unit>** for at least two channels. For detailed information about sensor settings, see section [Custom Sensors](#)³⁶⁴².

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) ³³⁸⁵ on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status** ¹⁹⁵¹. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) ³⁶⁸³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Escape Special Characters and Whitespaces in Parameters

 You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ":", "_", "-", "=", and "/" outside of quoted strings.

 We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#)³⁶⁵⁵ for details.

More

Information about custom scripts and executables

- [Custom Sensors](#)³⁶³⁷
- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵

Knowledge Base: What is the Mutex Name in the PRTG EXE/Script Sensor settings?

- <https://kb.paessler.com/en/topic/6673>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: How can I use meta-scans for custom EXE/Script sensors?

- <https://kb.paessler.com/en/topic/68109>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

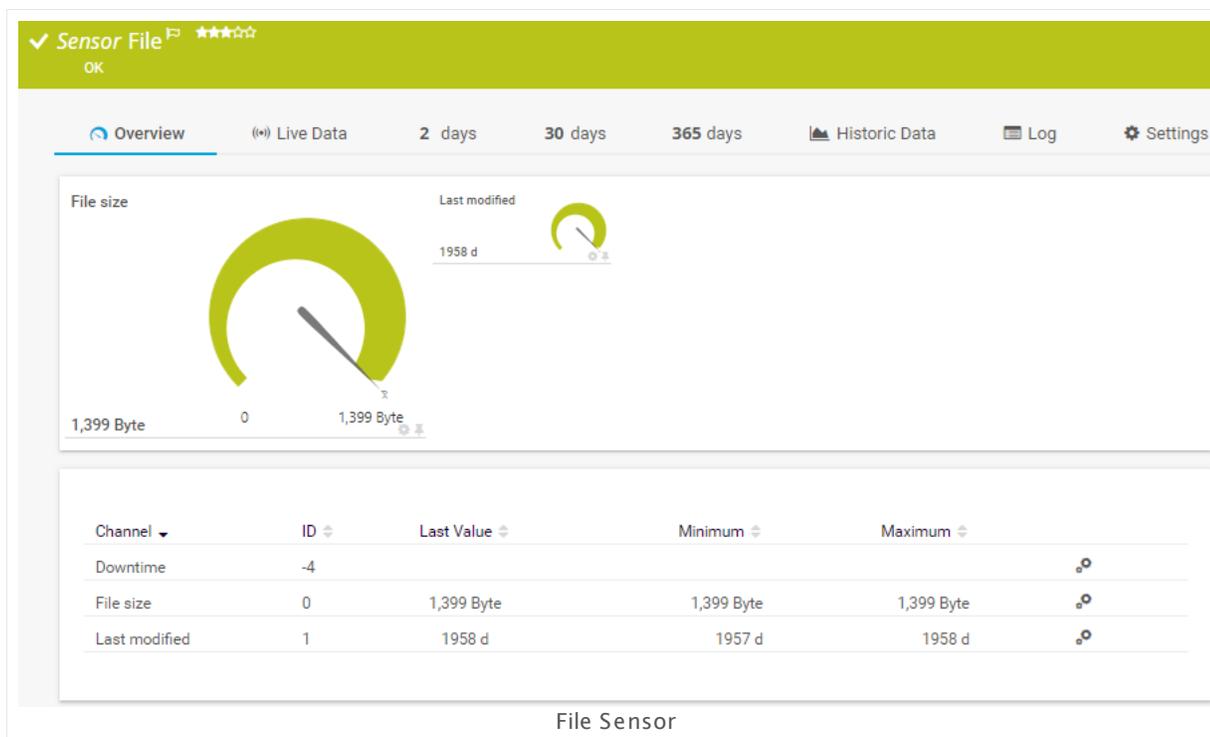
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.40 File Sensor

The File sensor monitors a file located on the local disk on the parent probe system, parent device, or a file accessible via Server Message Block (SMB). You can monitor changes to the file content and file time stamp.

It can show the following:

- File size
- Passed time since the file was modified the last time (in days, hours, and minutes, depending on the elapsed time)
- In contrast to the [Folder sensor](#)^[880], you can also monitor if the actual content of a specific file has changed.



Sensor in Other Languages

Dutch: **Bestand**, French: **Fichier**, German: **Datei**, Japanese: **ファイル**, Portuguese: **Arquivo**, Russian: **Файл**, Simplified Chinese: **文件**, Spanish: **Archivo**

Remarks

- [Requires](#)^[881] the LanmanServer ("Server") Windows service to be running on the target computer to monitor files on a share.
- Try using the Fully Qualified Domain Name (FQDN) of the target device if the sensor does not get a connection with the IP address.

- Knowledge Base: [What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032](#)
- Knowledge Base: [Can I use placeholders in file names to monitor log files?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

 To monitor files on Windows shares, please make sure the **LanmanServer** ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[213] , logs ^[228] , notifications ^[3216] , reports ^[3262] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SENSOR SPECIFIC

File Name	<p>Enter the full path to the file that this sensor will monitor. For example, enter <code>C:\Windows\file.txt</code> to monitor a file on the parent probe system.</p> <p>If you use a local path, the sensor will only look for the target file on the system on which the parent probe runs, not on the parent device! To monitor a file on the parent device, use the dollar sign (\$) like <code>C\$\User\johnqpublic\file.txt</code></p> <p>If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part: only enter <code>share\folder\file.txt</code>. The server part <code>\\server\</code> is taken from the parent device settings^[402] of this sensor. Enter a valid path and file name.</p> <p>i To provide any shares, the LanmanServer "Server" Windows service must be running on the target computer.</p>
Sensor Behavior	<p>Specify when the sensor shows a Down status^[195]. Choose between:</p> <ul style="list-style-type: none">▪ Show 'Down' status if file does not exist: The sensor will show an error if the file does not exist.▪ Show 'Down' status if file exists: The sensor will show an error if the file does exist.

SENSOR SPECIFIC

- Monitor File Content** Specify if the sensor will send a change notification when the content of the file changes (based on a checksum). Choose between:
- **Ignore changes:** No action will be taken on change.
 - **Trigger 'change' notification:** The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) 3170 whenever the sensor value changes.
- Monitor File Time Stamp** Specify if the sensor will send a change notification when the content of the file's time stamp changes. Choose between:
- **Ignore changes:** No action will be taken on change.
 - **Trigger 'change' notification:** The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) 3170 whenever the sensor value changes.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) 3160 settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <https://kb.paessler.com/en/topic/513>

Knowledge Base: Can I use placeholders in file names to monitor log files?

- <https://kb.paessler.com/en/topic/67965>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

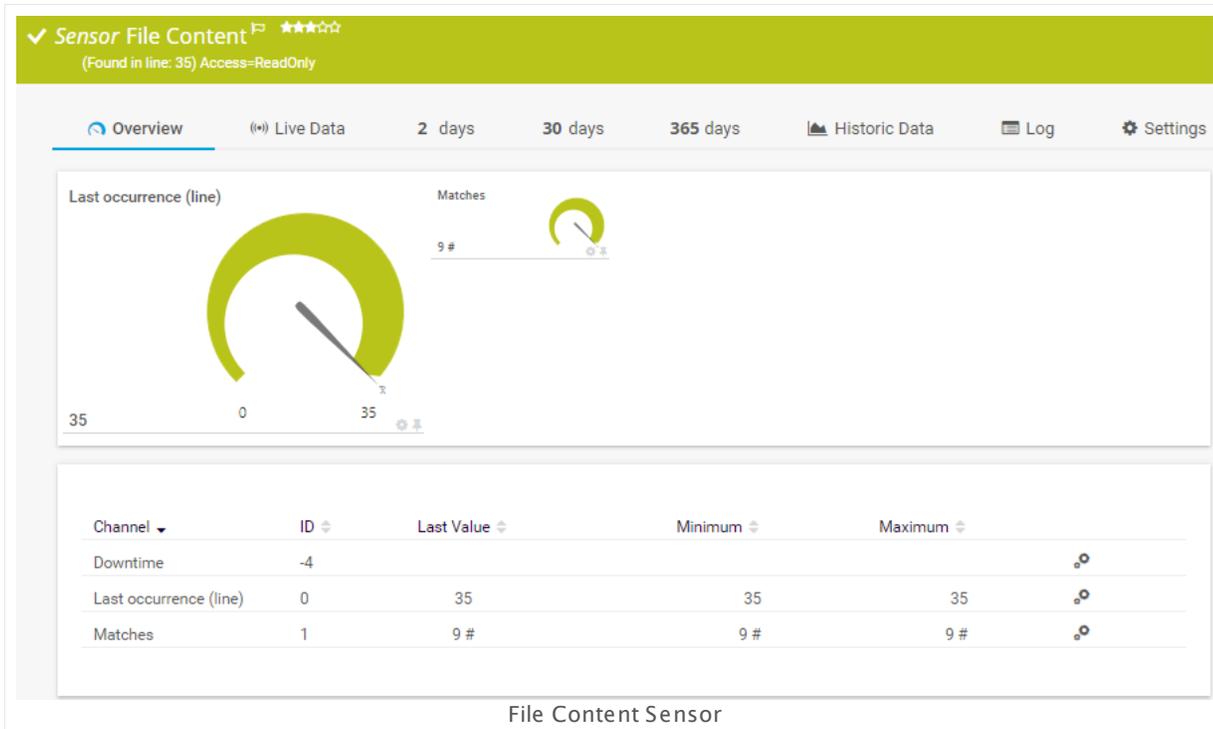
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.41 File Content Sensor

The File Content sensor checks a text file (for example, logfiles) for certain strings and returns the following:

- Line number of the last match
- Number of total matches.
- Additionally, the sensor quotes matching lines in the sensor message field.



Sensor in Other Languages

Dutch: **Bestands inhoud**, French: **Contenu du fichier**, German: **Dat ei-Inhalt**, Japanese: **ファイル内容**, Portuguese: **Conteúdo de arquivo**, Russian: **Содержимое файла**, Simplified Chinese: **??**, Spanish: **Contenido de archivo**

Remarks

- This sensor does not support UTF-16 encoded files! In this case, please try to use a custom sensor like the [EXE/Script Sensor](#)^[834] or the [EXE/Script Advanced Sensor](#)^[847].
- This sensor does not officially support binary files! If you would still like to monitor binary files contrary to our recommendation, then please choose the option **Always transmit to PRTG the entire file** in section **Network Usage** in the sensor settings.
- This sensor supports Unix line feeds.
- [Requires](#)^[871] the LanmanServer ("Server") Windows service to be running on the target computer to monitor files on a share.

- To monitor files on a Linux system, the folder has to be accessible via SMB.
- Try using the Fully Qualified Domain Name (FQDN) of the target device if the sensor does not get a connection with the IP address.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

 To monitor files on Windows shares, please make sure the **LanmanServer** ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SENSOR SPECIFIC

File Name	<p>Enter the full path to the file that this sensor will monitor. For example, enter <code>C:\Windows\file.txt</code>. to monitor a file on the parent probe system.</p> <p>If you use a local path, the sensor looks for the target file only on the system on which the parent probe runs, not on the parent device! To monitor a file on the parent device, use the dollar sign (\$) like <code>C\$\User\johnqpublic\file.txt</code>.</p> <p>If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part (only enter <code>share\folder\file.txt</code>). The server part (<code>\\server\</code>) is taken from the parent device settings^[402] of this sensor. Enter a valid path and file name.</p> <p> To provide any Windows shares, the LanmanServer "Server" Windows service must run on the target computer.</p> <p> To monitor any Linux files, the folder with these files has to be accessible via Server Message Block (SMB).</p> <p> Please be aware that it might produce high network traffic if you define PRTG to query an entire file on your network with every scanning interval.</p>
-----------	---

SENSOR SPECIFIC

Search String Define the string inside the logfile you want to check for. The input is not case-sensitive. Please enter a string.

Search Method Define the method you want to provide the search string with. The pattern must be in **one** line and only the **last** matching line will be given back. Choose between:

- **Simple string search:** Search for a simple plain text expression.
- **Regular Expression:** Search using a regular expression.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) ³⁷⁰⁴.

Network Usage Define in which way the sensor will transmit the target file to PRTG. Choose between:

- **Only transmit to PRTG new lines at the end of the file (default):** This option improves the performance of the sensor. It sends the whole file only with the first scan to PRTG. With the following sensor scans, the sensor will only transmit lines that were appended since the last scan. All other lines (that already existed in the previous scan) are not sent. The sensor assumes that they are unchanged and still counts them.

BETA This option is currently in beta status. Please do not expect that it will work as expected in every usage scenario!

- **Always transmit to PRTG the entire file:** The sensor sends the whole file with every sensor scanning interval to PRTG. If this results in too much traffic on the target system, we recommend that you choose the new lines option.

The sensor can only transmit newly added lines in the following cases:

- the file is bigger than at the previous scan, and
- the last line in the file at the previous scan still has to be at the same place in the file.

 The sensor supports Windows and Linux line endings (**CRLF** or **LF**).

File Encoding Specify the encoding of the file that this sensor monitors. Choose between:

- **Windows-1252**

SENSOR SPECIFIC

- UTF-8
- UTF-16

Warning Behavior

Define under which condition the sensor will show a **Warning status** ¹⁹⁵. Choose between:

- **Go into warning status when string is not found:** The sensor will show a **Warning** status if there is **no** match. Otherwise it will remain in **Up** status.
- **Go into warning status when string is found:** The sensor will show a **Warning** status if there **is** a match. Otherwise it will remain in **Up** status.

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) ³¹⁷⁰ whenever the sensor value changes.

 The change notification for this sensor is triggered if the value of the channel **Last occurrence (line)** changes. It is **not** triggered when the number of **Matches** changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#) ³⁷³⁴.

DEBUG OPTIONS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.42 Folder Sensor

The Folder sensor monitors a folder using Server Message Block (SMB). You can monitor file changes and file ages.

It can show the following:

- Folder size in bytes
- Number of files in the folder
- Passed time since the last change to a file in the folder ("newest file")
- Passed time since the oldest modification of a file in the folder ("oldest file")

i The Folder sensor counts all files in a folder, including **hidden files**.



Sensor in Other Languages

Dutch: **Map**, French: **Dossier**, German: **Ordner**, Japanese: フォルダー, Portuguese: **Pasta**, Russian: Папка, Simplified Chinese: ? ? ? , Spanish: **Carpeta**

Remarks

- This sensor counts all files in a folder, including hidden files.

- [Requires](#)⁸⁸¹ the LanmanServer ("Server") Windows service to be running on the target computer to monitor shares.
- Knowledge Base: [What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer ("Server") Windows Service

- ✘ To monitor shares on Windows machines, please make sure the **LanmanServer** ("Server") Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page. You can change the file age check later via the **Limits** section in the [channel settings](#)³¹⁶² of **Newest File** and **Oldest File**.

FOLDER MONITOR

Check of File Ages	<p>Specify if the sensor will monitor the folder for certain file ages and show a corresponding status¹⁹⁵. Choose between:</p> <ul style="list-style-type: none"> ▪ Don't check: Do not check for the age of the files in the specified folder(s). ▪ Show Warning if older: Set the sensor to Warning status if one of the files in the specified folder is older than a specific time unit. ▪ Show Error if older: Set the sensor to Down status if one of the files in the specified folder is older than a specific time unit. ▪ Show Warning if younger: Set the sensor to Warning status if one of the files in the specified folder is younger than a specific time unit. ▪ Show Error if younger: Set the sensor to Down status if one of the files in the specified folder is younger than a specific time unit.
--------------------	---

FOLDER MONITOR

File Age Limit	<p>This field is only visible if you enable a file age check above. Enter the age of a file in the folder that will trigger the sensor status change if the defined age is undercut respectively exceeded. Please enter an integer value.</p> <p>The value will be interpreted as days, hours, or minutes, according to your setting below.</p>
File Age Limit Unit	<p>This field is only visible if you enable a file age above. Specify the unit for the file age value that you entered above. Choose between:</p> <ul style="list-style-type: none"> • In days: Choose this option if you entered a number of days in the field above. • In hours: Choose this option if you entered a number of hours in the field above. • In minutes: Choose this option if you entered a number of minutes in the field above.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	<p>Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree^[181], as well as in alarms^[219], logs^[228], notifications^[3216], reports^[3252], maps^[3278], libraries^[3235], and tickets^[230].</p>
Parent Tags	<p>Shows Tags^[139] that this sensor inherits^[140] from its parent device, group, and probe^[133]. This setting is shown for your information only and cannot be changed here.</p>

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

FOLDER MONITOR

Folder Name	<p>Enter the full path to the folder this sensor will monitor. For example, enter <code>C:\Windows</code>.</p> <p>If the file is located on a network device, use the Uniform Naming Convention (UNC) path without the server part (you would only enter <code>share\folder</code>). The server part (<code>\\server\</code>) is taken from parent device settings^[402] of this sensor. Please enter a valid path name.</p> <p> To monitor shares, the LanmanServer "Server" Windows service must be running on the target computer.</p>
Subfolder Recursion	<p>Specify if the sensor will include subfolders in the folder monitoring. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not recurse subfolders: Only monitor the folder specified above and do not monitor its subfolders. ▪ Monitor the folder and its subfolders (use with caution!): Monitor the folder specified above and all of its subfolders. <ul style="list-style-type: none">  Recursing subfolders in large directories with a high number of branches may evoke timeout errors or performance issues.
Monitor Folder Changes	<p>Specify if the sensor will send a change notification when the content of the folder changes. Choose between:</p>

FOLDER MONITOR

- **Ignore changes:** Changes to the folder will not trigger a change notification.
- **Trigger 'On Change' notification:** The sensor will trigger a change notification if a file changes its timestamp or filename, or if there are new or deleted files. [Create a change trigger](#)³¹⁸⁰ on the **Notification Triggers** tab of this sensor to receive a notification whenever there is a change.

Timeout

Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[320] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <https://kb.paessler.com/en/topic/513>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

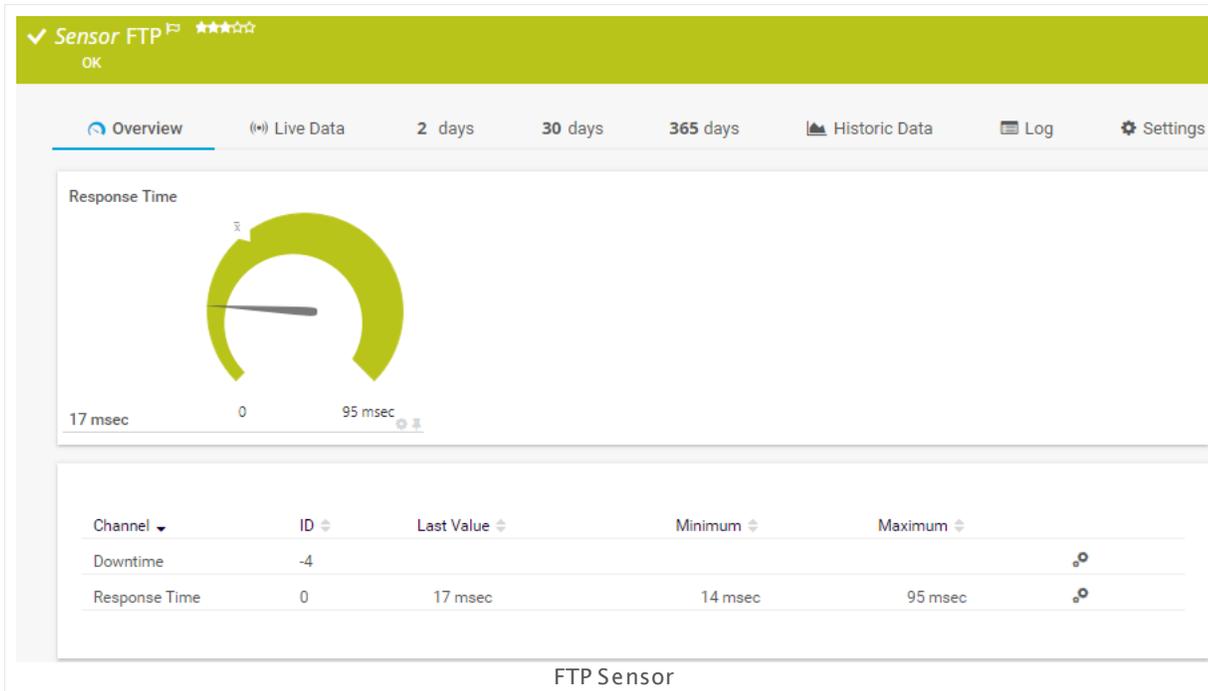
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.43 FTP Sensor

The FTP sensor monitors file servers using File Transfer Protocol (FTP) and FTP over SSL (FTPS). It can show the following:

- Response time of the server
- Response message of the server



Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	<p>Enter the number of the port the sensor tries to connect to. Please enter an integer value. We recommend that you use the default value.</p> <p>If you cannot make a connection, please try another port number.</p>
FTP Mode	<p>Define the FTP connection mode that the sensor will use for the connection to FTP server. Choose between:</p> <ul style="list-style-type: none"> ▪ Use active mode

SENSOR SPECIFIC

- **Use passive mode**

 We recommend that you use the default value. If you cannot establish a connection, please try the passive mode.

TRANSPORT-LEVEL SECURITY

FTP Specific

Specify if the sensor uses encryption for the connection. Choose between:

- **Use Transport-Level Security if available:** The sensor tries to connect via TLS. It determines automatically whether to connect via explicit or implicit mode. If TLS is not supported by the server, the sensor will try connecting without encryption and show an **Up** status if this works.
 - **Enforce Transport-Level Security:** The connection **must** be established using TLS (explicit or implicit mode). Otherwise, the sensor will show a **Down** status.
 - **Do not use Transport-Level-Security:** The sensor connects to the FTP server without encryption.
-  You can see in the sensor logs which method the sensor used previously to connect to the FTP server.

AUTHENTICATION

Username

Enter a username for the FTP login. Please enter a string or leave the field empty.

 Default username is "anonymous". If the sensor cannot log into the FTP server with this username (or another one that you define), the sensor message will show that the credentials are incorrect but the sensor will remain in **Up** status.

Password

Enter a password for the FTP login. Please enter a string or leave the field empty.

 If the sensor cannot log onto the FTP server with this password, the sensor message will show that the credentials are incorrect but the sensor will remain in **Up** status.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[310] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

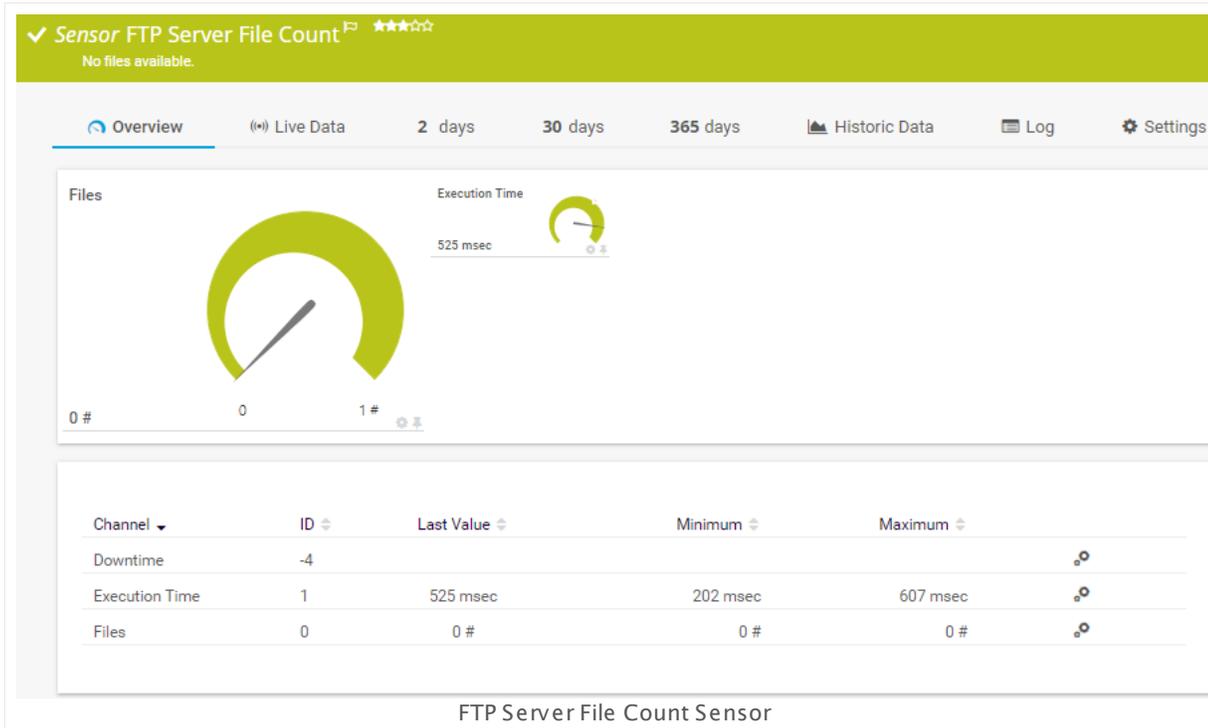
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.44 FTP Server File Count Sensor

The FTP Server File Count sensor logs in to an File Transfer Protocol (FTP) server and can monitor changes to files.

- It can show the number of files available in the directory listing.



Sensor in Other Languages

Dutch: **FTP Server File Aantal**, French: **Nombre de fichiers du serveur FTP**, German: **FTP-Server Dateienanzahl**, Japanese: **FTP サーバファイルカウント**, Portuguese: **Contagem de arquivos no FTP**, Russian: **Количество файлов на FTP-сервере**, Simplified Chinese: **FTP 服务器文件数量**, Spanish: **Número de archivos en el servidor FTP**

Remarks

- [Requires](#) .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

FTP Mode Define the FTP connection mode that the sensor will use for the connection to FTP server. Choose between:

- **Use active mode**
- **Use passive mode**

i We recommend that you use the default value. If you cannot establish a connection, please try the passive mode.

Check Method Define how to access the FTP server directory that this sensor monitors. Choose between:

- **Check URL:** The sensor uses an explicitly defined URL of an FTP server to access the target directory.
- **Check folder on parent device:** The sensor uses the IP address or DNS name of the parent device where you add this sensor to and monitors a defined folder on this device.

FTP URL This field is only visible if you select the URL method above. Enter the URL that this sensor checks. The URL can look like this:
`ftp://10.0.0.1/upload`

i If you use this method, this sensor will **not** use the **IP Address/DNS value** of the parent device.

i You can add a port number to the URL by using a colon, for example, `ftp://10.0.0.1/upload:21`

SENSOR SETTINGS

FTP Port	This field is only visible if you select the parent device method above. Enter the number of the port to which this sensor connects. Default port is 21 .
FTP Folder	This field is only visible if you select the parent device method above. Enter the name of the folder on the parent device that this sensor monitors, for example: upload
Subfolder Recursion	<p>This field is only visible if you select the parent device method above. Define if the sensor additionally monitors the subfolders of the FTP folder you specify above. Choose between:</p> <ul style="list-style-type: none">▪ Do not recurse subfolders: The sensor monitors only the folder that you define above and ignores its subfolders.▪ Monitor the folder and its subfolders (use with caution!): The sensor recursively checks all subfolders in addition to the folder that you define above.  Recursing subfolders in large directories with a high number of branches may evoke timeout errors or performance issues.
Username	Enter the username for the login to the FTP server. Please enter a string.
Password	Define the password for the login to the FTP server. Please enter a string.
File Count	<p>Define which file the sensor counts. Choose between:</p> <ul style="list-style-type: none">▪ Count the total number of files: The sensor always shows the total number of all files in the defined folder.▪ Count only new files: The sensor shows only the number of new files since the last sensor scan. You can define the frequency of sensor scans in section Scanning Interval ⁹⁰⁵.  With every sensor scan, any new files from the previous scan will be regarded as old.
Security	<p>Define the the encryption of the connection. Choose between:</p> <ul style="list-style-type: none">▪ Do not use an encryption: The sensor connects without encryption.▪ Use explicit SSL: The sensor establishes the connection to the FTP server via SSL.  This sensor type only supports explicit SSL.

SENSOR SETTINGS

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) ³⁷⁷⁰ whenever the sensor value changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#) ³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

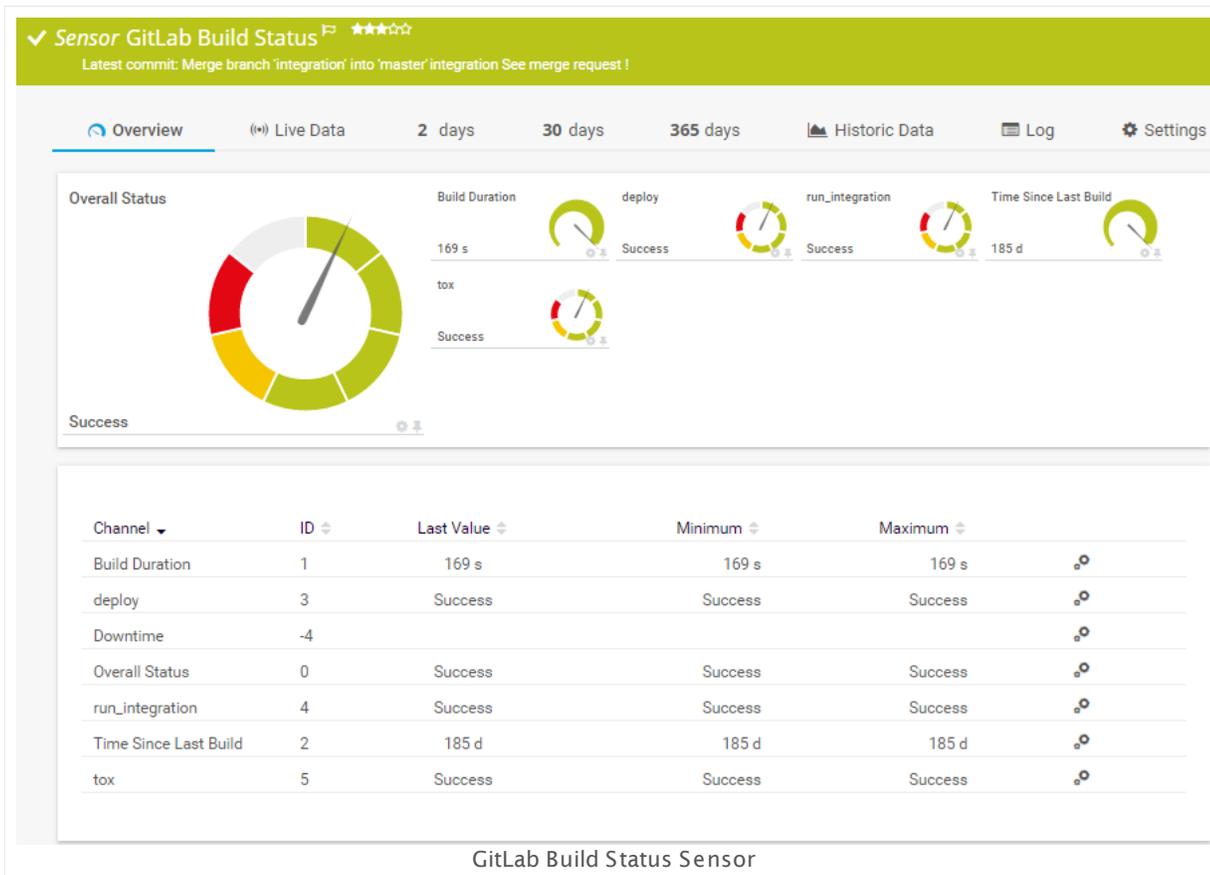
7.8.45 GitLab Build Status Sensor

The GitLab Build Status sensor monitors the status of the latest build on one specific branch. You can monitor your builds in either your own GitLab environment or on [GitLab.com](https://gitlab.com).

It can show the following:

- Overall status of the latest build (unknown, success, pending, canceled, failed)
- Duration of the latest build
- Time since the last build
- Status of the different build steps

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **GitLab Build Status**, French: **État de build de GitLab**, German: **GitLab Buildstatus**, Japanese: **GitLabビルドステータス**, Portuguese: **Estado do build no GitLab**, Russian: **Статус сборки GitLab**, Simplified Chinese: **GitLab ? ? ? ?**, Spanish: **Estado de compilación de GitLab**

Remarks

- The sensor uses the IP or DNS address of the parent device to find the GitLab server. To monitor branches in the GitLab cloud, enter **gitlab.com** as address in the [parent device settings](#)^[402].
- The sensor can only monitor builds that are using **GitLab Continuous Integration (CI)**. Builds using external CI tools (for example, **Jenkins**) are not supported.
- Use with care! This sensor has high impact on the performance of your GitLab server. Please do not add too many sensors of this type to your GitLab server, only monitor the most important branches.
- We do not recommend to add this sensor for temporarily existing branches. This is not useful in most cases.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The sensor requires an **Access Token** to access your projects on GitLab. Before you can actually create the sensor, it will ask you for this token. You can create it on the GitLab web interface in your profile under **Profile Settings | Access Token**. Copy the created token and paste it into the **GitLab Access Token** field in the **GitLab Credentials** dialog of the sensor.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GITLAB REPOSITORY

Branch	Select the branches you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------	--

GITLAB REPOSITORY

To better find what you want to monitor, especially in large tables, use the search function in the upper right corner. For example, you can filter for a specific project to show related branches only.

i The sensor scans the last 100 builds of all projects during sensor creation (meta-scan). If you miss a branch in the overview, start a build on the branch that is missing and add the sensor anew.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GITLAB CREDENTIALS

GitLab Access Token Enter the **Access Token** that you have defined in your GitLab profile. You can create the token on the GitLab web interface in your profile under **Profile Settings | Access Token**.

By default, this field show the access token that you have provided during sensor creation.

GITLAB REPOSITORY

Project ID These fields show various information about the project and branch that this sensor monitors.

Project Name

Branch

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

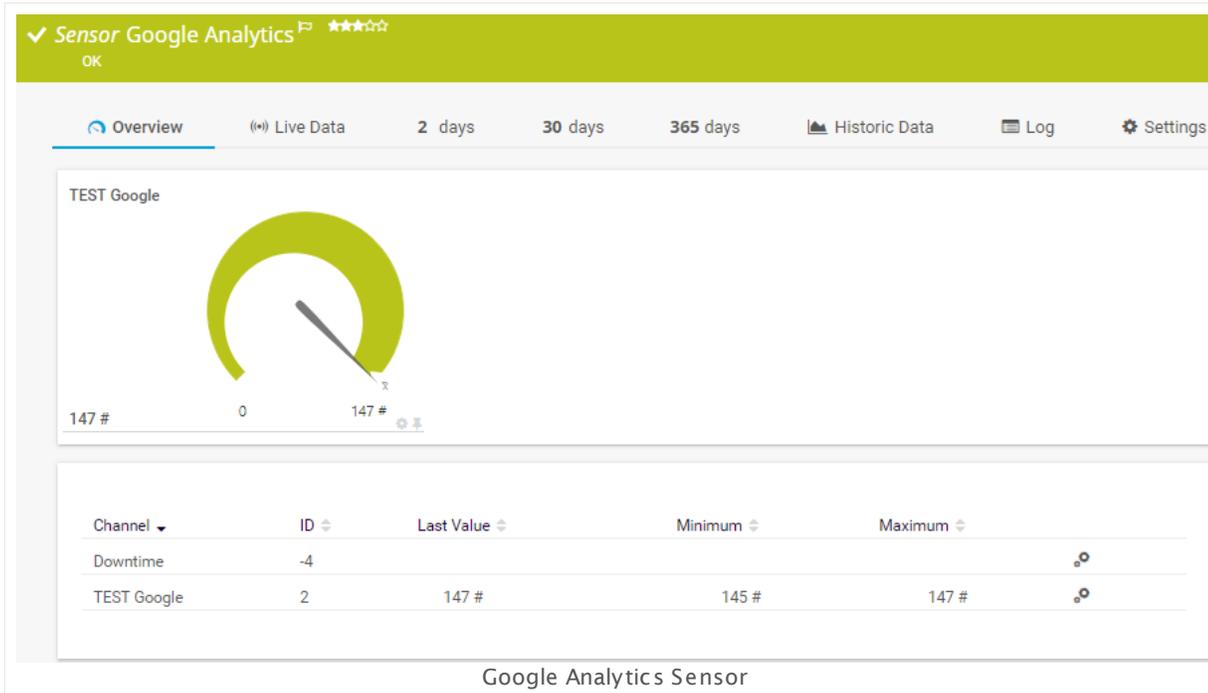
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.46 Google Analytics Sensor

The Google Analytics sensor queries and monitors several metrics from a Google Analytics account using the Google Application Programming Interface (API) and [OAuth2](#).

- It can show the values for all available Google Analytics metrics in different sensor channels.



Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, see manual section [Authentication Using OAuth2](#).
- Some dimensions and metrics cannot be queried together. See the Knowledge Base: [Where do I find available Google Analytics metrics?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- X** PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GOOGLE CREDENTIALS

This sensor type uses **OAuth2** authentication to get access to your Google account. For details about the authentication approach, see section [Authentication Using OAuth2](#)⁹³².

OAuth URL Click the **Get Access Code** button to connect this sensor to your Google Analytics account using OAuth2. This is necessary to allow the sensor to query data from Google Analytics. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your Google Analytics account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.

OAuth Code Paste the access code that you receive after completing the authorization process for PRTG at your Google Analytics account. Click **OK** to define the [sensor settings](#)⁹²³.

i It is mandatory to connect this sensor to your Google Analytics account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

GOOGLE ANALYTICS SPECIFIC

Profile Choose the Google Analytics profile that you want to monitor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #2 - #10 You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for **Sensor Channel #1** without enabling it manually. Additionally you can define **Sensor Channel #2** up to **Sensor Channel #10**. To do so, choose between:

- **Disable:** The sensor will not create this channel.
- **Enable:** Create an additional channel and define all its characteristics below (name, metric, mode, and unit).

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

GOOGLE ANALYTICS SPECIFIC

 It is not possible to enable or disable sensor channels after the creation of this sensor!

Channel #x Mode

Define how to display the retrieved value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended):** Shows the value as the sensor retrieves it from Google Analytics.
- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from Google Analytics. This mode is not compatible with the unit **Value Lookup**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GOOGLE CREDENTIALS

OAuth Code Shows the authorization code that the sensor uses to get access to your Google Analytics account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

GOOGLE ANALYTICS SPECIFIC

Profile Shows the Google Analytics profile that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Time Span Define the time that the queried monitoring covers. Choose between:

- **Last week (default)**
- **Yesterday**
- **Today**

Sensor Channel #x Name Enter a name for the channel in which the sensor shows the results for the metric you choose below. Please enter a string.

Sensor Channel #x Metric Select a metric that you want to monitor. You can choose between available Google Analytics. If your desired metric is not listed, choose **Custom Metric** and specify below.

GOOGLE ANALYTICS SPECIFIC

Sensor Channel #x Custom Metric This field is only visible if you choose custom metric above. Enter the identifier of the metric that you want to monitor. Type it exactly as shown in Google Analytics. Metric identifiers always start with **ga:**

Please enter a string.

Sensor Channel #x Mode Shows how the sensor displays the retrieved value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Unit Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

For more information about the available units, see section [Custom Sensors](#)³⁶⁴².

i To use [lookups](#)³⁶⁹³ with this channel, choose the unit **Value Lookup** and select your lookup file below. Do not use the unit **Custom** for using lookups with this sensor and do not use the [channel settings](#)³¹⁰⁰ to define a lookup file!

GOOGLE ANALYTICS SPECIFIC

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit This setting is only visible if you select the **Custom** unit option above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x
Value Lookup This setting is only visible if you select the **Value Lookup** option above. Choose a [lookup](#) file that you want to use with this channel.

Sensor Channel #x Shows if you enabled or disabled a channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

 You can define up to 10 different sensor channels per sensor.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- ⓘ If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- ⓘ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

ⓘ This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

ⓘ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

ⓘ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p> To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Authentication Using OAuth2

 This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. Authorization Request

First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. Verifying Identity

This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.

 If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. Authorizing PRTG

Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. Getting Authorization Code

Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.

-  The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. Providing Authorization Code

Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. Requesting Access Token

After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access tokens are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. Retrieving Data

The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

More

Knowledge Base: Where do I find available Google Analytics metrics?

- <https://kb.paessler.com/en/topic/35373>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

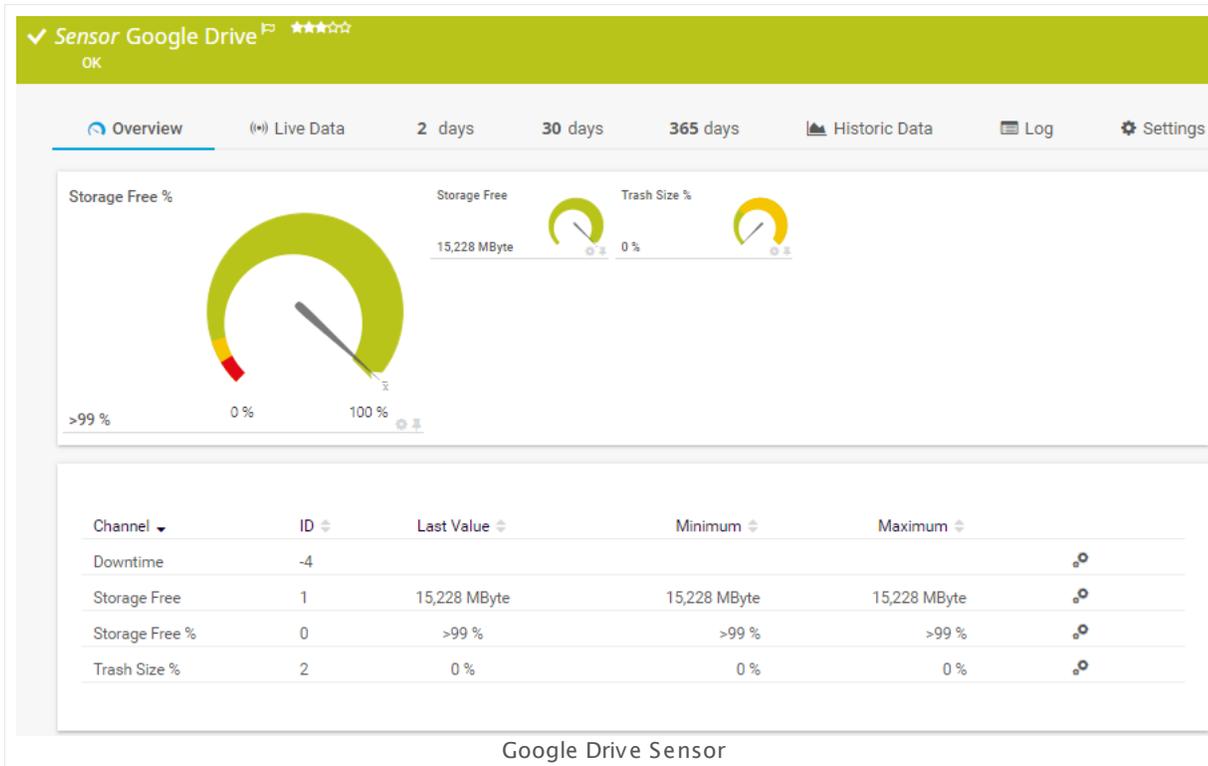
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.47 Google Drive Sensor

The Google Drive sensor monitors a Google Drive account using the Google Application Programming Interface (API) and [OAuth2](#). It shows the following:

- Free storage in bytes and percent
- Trash size in percent



Sensor in Other Languages

Dutch: **Google Drive**, French: **Google Drive**, German: **Google Drive**, Japanese: **Google ドライブ**, Portuguese: **Google Drive**, Russian: **Google Диск**, Simplified Chinese: **Google Drive**, Spanish: **Google Drive**

Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, see manual section [Authentication Using OAuth2](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- ✘ PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

GOOGLE CREDENTIALS

This sensor type uses **OAuth2** authentication to get access to your Google account. For details about the authentication approach, see section [Authentication Using OAuth2](#)^[942].

OAuth URL Click the **Get Access Code** button to connect this sensor to your Google Drive account using OAuth2. This is necessary to allow the sensor to query data from Google Drive. A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your Google Drive account. Copy the OAuth code you get and paste it into the **OAuth Code** field below.

OAuth Code Paste the access code that you receive after completing the authorization process for PRTG at your Google Drive account. Click **OK** to define the [sensor settings](#)^[935].

i It is mandatory to connect this sensor to your Google Drive account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

GOOGLE CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your Google Drive account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Authentication Using OAuth2

 This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. Authorization Request

First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. Verifying Identity

This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.

 If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. Authorizing PRTG

Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. Getting Authorization Code

Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.

-  The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. Providing Authorization Code

Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. Requesting Access Token

After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access tokens are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. Retrieving Data

The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

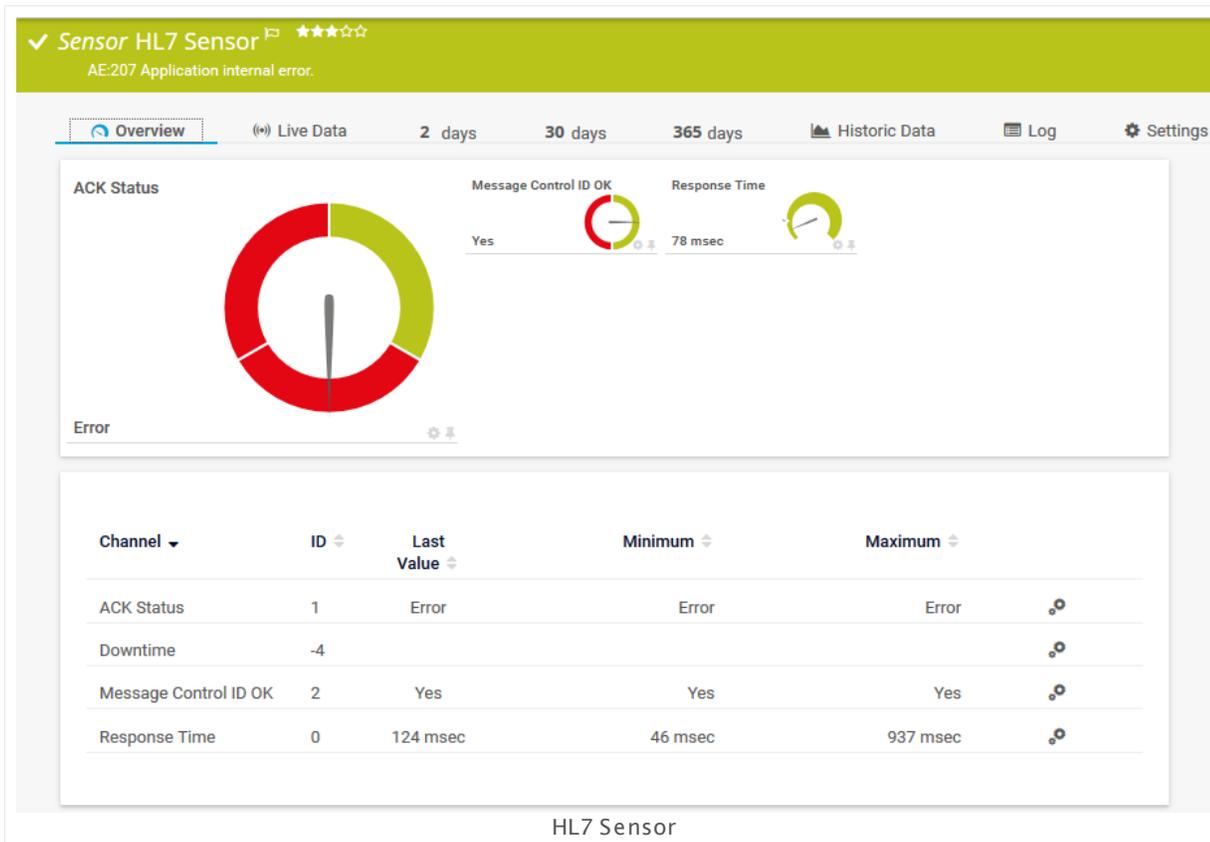
7.8.48 HL7 Sensor

The HL7 sensor monitors the availability of HL7 interfaces. It sends an HL7 message to the target device and checks for a valid response.

The sensor shows the following:

- Acknowledgment (ACK) status
 - **Up status** ¹⁹⁵ for accepted messages
 - **Down status** for rejected messages or errors
- Message control ID status
- Response time

You can define your own messages in HL7 format as **.hl7** files in the [PRTG program directory](#) ³⁷⁴. The sensor sends them to the HL7 capable system with each sensor scan.



Remarks

- [Requires](#) ⁹⁴⁵ .NET 4.6 or later on the probe system.

- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.6 or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HL7 MESSAGE SPECIFIC

HL7 Messages

Select an HL7 file from the list. The sensor will send it to the target device with every scanning interval.

The list shows all files available in the corresponding **\Custom Sensors\hl7** sub-directory of the probe system's PRTG program directory (see [Data Storage](#)³⁷³⁴). To appear in this list, please store the files into this folder ending in HL7.

To be accepted by the HL7 interface, your files must have the expected HL7 message format.

PRTG comes with two sample HL7 message files by default that you can use to test your HL7 monitoring and to have a look at the expected format. They are located in the **\Custom Sensors\hl7** folder.

HL7 MESSAGE SPECIFIC

You can override certain headers using the **Message Header (MSH)** sensor setting.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HL7 CONNECTION

Port	Enter the port of the HL7 interface that is used for the connection.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

HL7 MESSAGE SPECIFIC

Message Header (MSH)	<p>Define if you want to use the default message headers (MSH) as defined in the selected HL7 message file or if you want to override certain headers. Choose between:</p> <ul style="list-style-type: none">▪ Default MSH: Send the MSH as defined in the HL7 message file.▪ Override MSH: Define custom MSH below that will override the MSH in the HL7 message file.
Sending Application	<p>This field is only available if you choose to override the MSH above. Enter the name of the sending application, for example, PRTG. It will override the default value in the message.</p> <p>Please enter a string.</p>
Sending Facility	<p>This field is only available if you choose to override the MSH above. Enter the name of the sending facility. It will override the default value in the message.</p> <p>Please enter a string.</p>
Receiving Application	<p>This field is only available if you choose to override the MSH above. Enter the name of the receiving application. It will override the default value in the message.</p> <p>Please enter a string.</p>
Receiving Facility	<p>This field is only available if you choose to override the MSH above. Enter the name of the receiving facility. It will override the default value in the message.</p> <p>Please enter a string.</p>

HL7 MESSAGE SPECIFIC

HL7 Message	Shows the HL7 message file that the sensor uses to send the message with each scan. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------	--

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📁 For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

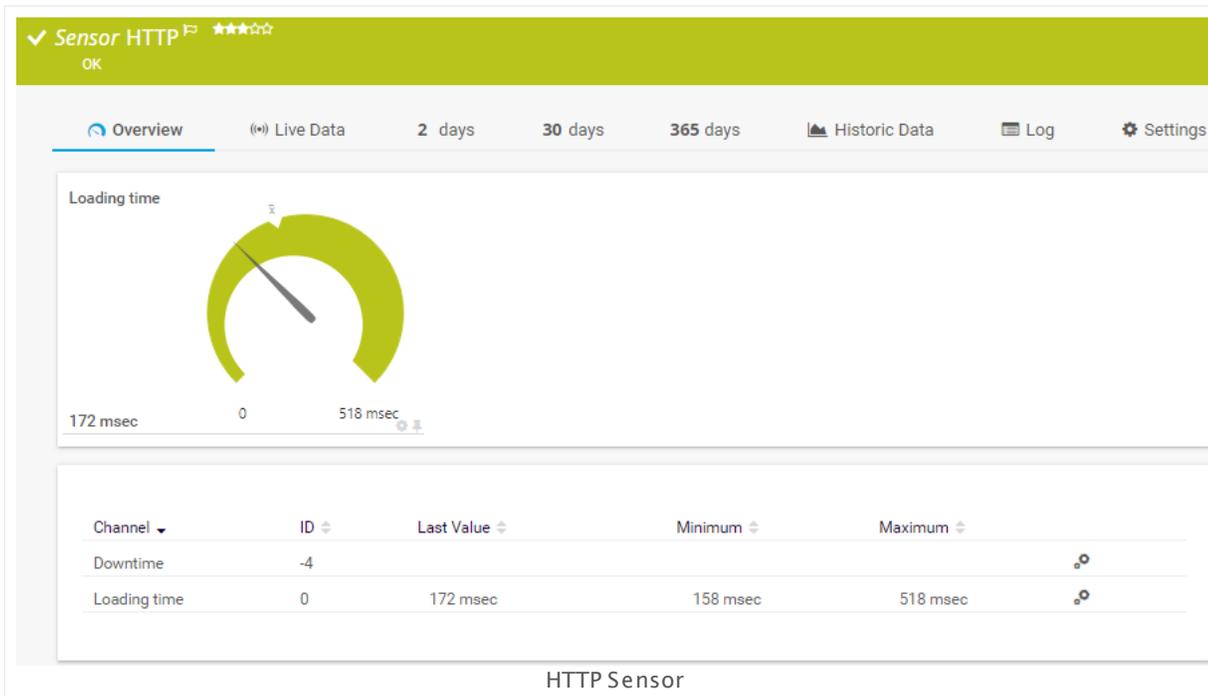
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.49 HTTP Sensor

The HTTP sensor monitors a web server using Hypertext Transfer Protocol (HTTP). This is the easiest way to monitor if a website (or a specific website element) is reachable.

- It shows the loading time of a web page or element.



Remarks

- Knowledge Base: [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	<p>Enter the URL the sensor connects to. It has to be URL encoded!</p> <p>If you enter an absolute URL, the sensor uses this address independently from the IP Address/DNS Name setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time.</p>

HTTP SPECIFIC

 PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Request Method

Choose an HTTP request method to determine how the sensor will request the given URL.

- **GET:** Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST:** Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.
- **HEAD:** Only request the HTTP header from the server without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata

This field is only visible when you select the **POST Request Method** setting above. Enter the data part for the POST request here.

 No XML is allowed here!

Content Type

This setting is only visible when you select the **POST Request Method** setting above. Define the content type of a POST request. Choose between:

- **Default (application/x-www-form-urlencoded):** This is the default content type used to encode the form data set for submission to the server.
- **Custom:** If you need another content type than default, enter this content type below.

Custom Content Type

This field is only visible when you select **Custom** above. Define the content type that is needed, for example, XML, JSON, HTTP.

Server Name Indication

Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the [parent device](#)⁴⁰² or the target URL of the sensor. SNI has to be a **Fully Qualified Domain Name (FQDN)**. Please ensure it matches the configuration of the target server.

 For details, see the Knowledge Base article [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)

HTTP SPECIFIC

- SNI Inheritance** Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the **Server Name Indication** setting above which SNI is determined. Choose between:
- **Inherit SNI from parent device:** The sensor determines the SNI from the host address of the parent device.
 - **Do not inherit SNI from parent device:** The sensor determines the SNI from the target **URL** as defined in the settings of this sensor.

i This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

- Graph Type** Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)

- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

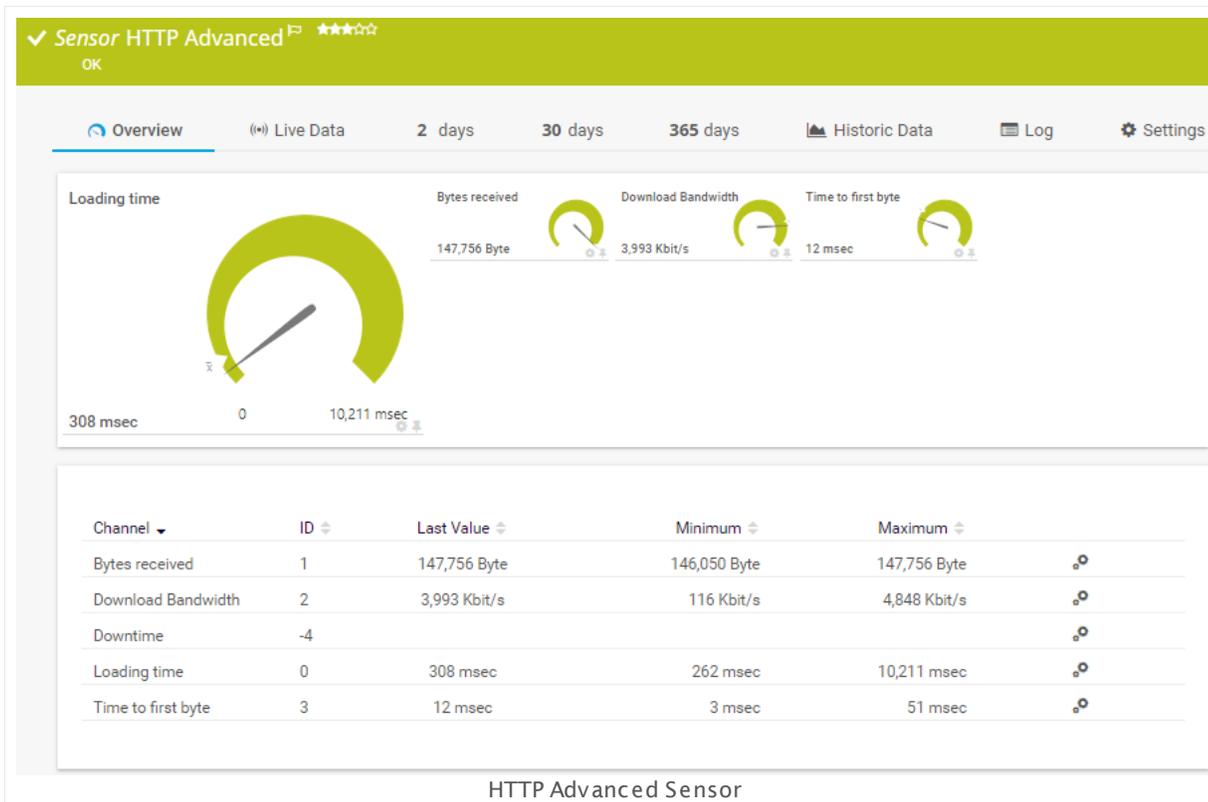
For more general information about settings, see the [Object Settings](#)²¹⁷¹ section.

7.8.50 HTTP Advanced Sensor

The HTTP Advanced sensor monitors the source code of a web page using Hypertext Transfer Protocol (HTTP). It supports authentication, content checks, and other advanced parameters.

The sensor can show the following:

- Loading time
 - Bytes received
 - Download bandwidth (speed)
 - Time to first byte
- ⓘ The monitored content size is uncompressed.



Sensor in Other Languages

Dutch: **HTTP Geavanceerd**, French: **HTTP (avancé)**, German: **HTTP (Erweitert)**, Japanese: **HTTP アドバンスド**, Portuguese: **HTTP avançado**, Russian: **HTTP (Расширенный)**, Simplified Chinese: **HTTP 高级**, Spanish: **HTTP Avanzado**

Remarks

- Supports [Smart URL Replacement](#)⁹⁸⁰.

- Knowledge Base: [Which user agent should I use in the HTTP Advanced sensor's settings?](#)
- Knowledge Base: [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- If you need to use SRP ciphers, please choose the **Alternate/Compatibility Mode** in the sensor settings.
- Bandwidth monitoring of fast internet connections may be inaccurate.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

URL Enter the URL the sensor connects to. It has to be **URL encoded!**

If you enter an absolute URL, the sensor uses this address independently from the **IP Address/DNS Name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time.

 PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Request Method Choose an HTTP request method to determine how the sensor will request the given URL.

- **GET:** Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST:** Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Post data** field below.
- **HEAD:** Only request the HTTP header from the server without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

HTTP SPECIFIC

Postdata	<p>This field is only visible when you select the POST Request Method setting above. Enter the data part for the POST request here.</p> <p> No XML is allowed here!</p>
Content Type	<p>This setting is only visible when you select the POST Request Method setting above. Define the content type of a POST request. Choose between:</p> <ul style="list-style-type: none"> ▪ Default (application/x-www-form-urlencoded): This is the default content type used to encode the form data set for submission to the server. ▪ Custom: If you need another content type than default, enter this content type below.
Custom Content Type	<p>This field is only visible when you select Custom above. Define the content type that is needed, for example, XML, JSON, HTTP.</p>
Server Name Indication	<p>Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the parent device or the target URL of the sensor. SNI has to be a Fully Qualified Domain Name (FQDN). Please ensure it matches the configuration of the target server.</p> <p> For details, see the Knowledge Base article My HTTP sensors fail to monitor websites which use SNI. What can I do?</p>
SNI Inheritance	<p>Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the Server Name Indication setting above which SNI is determined. Choose between:</p> <ul style="list-style-type: none"> ▪ Inherit SNI from parent device: The sensor determines the SNI from the host address of the parent device. ▪ Do not inherit SNI from parent device: The sensor determines the SNI from the target URL as defined in the settings of this sensor.

HTTP ENGINE

Monitoring Engine	<p>If you encounter unexpected errors with the standard method that is used to monitor a URL, try to use the compatibility mode, which is based on .NET. Choose between:</p>
-------------------	---

HTTP ENGINE

- **Default/High Performance (recommended):** This is the default monitoring method for this sensor type.
- **Alternate/Compatibility Mode:** Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor executes an external `exe`. Because of this, this method needs more resources, but it can be helpful in particular cases.
 - ⓘ If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below.
 - ⚠ When using the Compatibility Mode, **Smart URL Replacement** will not work, so this sensor will **not** use the **IP Address/DNS value** of the parent device automatically then.

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

SSL Method	<p>When using the compatibility mode, the SSL specific settings are a bit different to the default (automatically used) SSL settings. You can choose between:</p> <ul style="list-style-type: none"> ▪ SSL 3.0 ▪ TLS 1.0, TLS 1.1, TLS 1.2 ▪ SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 This is the default setting.
Check SSL Certificates	<p>Specify if the sensor will check the certificate of the monitored URL. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not check used certificates: Do not consider the certificates of the monitored web pages. This the default setting. ▪ Check if the used certificates are trusted: Inspect the certificates. If the certificate of the server is not trusted, the sensor shows a Down status and displays a corresponding message.

- ⓘ This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

Protocol Version	<p>Define the HTTP protocol version that the sensor will use when connecting to the target URL. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP 1.0 ▪ HTTP 1.1: This is the default setting.
User Agent	<p>Choose which user agent string the sensor will send when connecting to the target URL. Choose between:</p> <ul style="list-style-type: none"> ▪ Use PRTG's default string: Do not enter a specific user agent, use the default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows) ▪ Use a custom string: Use a custom user agent. Define below.
Custom User Agent	<p>This field is only visible if you enable custom user agent above. Enter a string to be used as user agent when connecting to the URL specified above.</p>
Use Custom HTTP Headers	<p>Define if you want to send custom HTTP headers to the target URL. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not use custom HTTP headers ▪ Use custom HTTP headers
Custom HTTP Headers	<p>This field is only available if you select using custom headers above. Enter a list of custom HTTP headers with their respective values that you want to transmit to the URL you define above, each pair in one line. The syntax of a header-value pair is header1:value1</p> <p> The sensor does not support the header field names user-agent, content-length, host.</p> <p> Ensure the HTTP header statement is valid! Otherwise, the sensor request will not be successful.</p>

Content Changes	<p>Define what the sensor will do if the content of the monitored web page (element) changes. You can choose between:</p> <ul style="list-style-type: none"> • Ignore changes: No action will be taken on change. • Trigger 'change' notification: The sensor will send an internal message indicating that the web page content has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification^[3170] whenever the web page content changes.
-----------------	---

Require Keyword	<p>Define if the sensor will check the result at the configured URL for keywords. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not check for keyword (default): Do not search for keywords in the result returned at the URL. ▪ Set sensor to warning if keyword is missing: Check if a keyword exists in the result and set the sensor to a Warning status ^[195] if yes. ▪ Set sensor to error if keyword is missing: Check if a keyword exists in the result and set the sensor to a Down status ^[195] if yes. <p> The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.</p>
Response Must Include	<p>This field is only visible if you enable keyword checking above (include). Define which string must be part of the source code at the given URL. You can either enter plain text or a Regular Expression ^[3704]. Specify below.</p> <p>If the data does not include the search pattern, the sensor will show the status defined above. Please enter a string.</p>
Check Method	<p>Define the format of the search expression in the field above.</p> <ul style="list-style-type: none"> ▪ String search (default): Search for the string as plain text. The characters * and ? work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. You can also search for HTML tags. ▪ Regular Expression: Use the search pattern as a Regular Expression ^[3704]. <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions ^[3704].</p>
Exclude Keyword	<p>Define if the sensor will check the result at the configured URL for keywords. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not check for keyword (default): Do not search for keywords in the result returned at the URL. ▪ Set sensor to warning if keyword is found: Check if a keyword exists in the result and set the sensor to a Warning status ^[195] if yes.

	<ul style="list-style-type: none"> ▪ Set sensor to error if keyword is found: Check if a keyword exists in the result and set the sensor to a Down status ^[195] if yes. <p> The content check is only intended for HTML websites and might not work with other target URLs. For example, binary files are not supported.</p>
Response Must Not include	This field is only visible if you enable keyword checking (exclude) above. Define which string must not be part of the source code at the given URL. You can either enter plain text or a Regular Expression ^[3704] . If the data does include this string, the sensor will show the status defined above. Please enter a string.
Check Method	Define in which format you have entered the search expression in the field above. <ul style="list-style-type: none"> ▪ String Search (default): Search for the string as plain text. The characters asterisk (*) and question mark (?) work here as placeholder, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search. You can also search for HTML tags. ▪ Regular Expression: Use the search pattern as a Regular Expression ^[3704]. <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions ^[3704].</p>
Limit Download (kb)	Enter a maximum amount of data that the sensor can transfer per every single request. If you set content checks, please be aware that only the content downloaded up to this limit can be checked for search expressions.
Result Handling	Define what the sensor will do with the data loaded at the given URL. Choose between: <ul style="list-style-type: none"> • Discard HTML result: Do not store the requested data. • Store latest HTML result: Store the last result of the requested data to the Logs (Sensors) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval. <p> For information on how to find the folder used for storage, see section Data Storage ^[3734].</p>

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

-  This sensor loads the source code at the given URL. If you set up a content check, only this source code is checked for the keywords. The code is not necessarily identical to the one used to display the page when opening the same URL in a web browser, as there may be a reload configured or certain information may be inserted after loading, for example, via JavaScript.
-  PRTG does not follow links to embedded objects nor does it execute scripts. Only the first page at the given URL is loaded and checked against the expressions configured.
-  For debugging, please use the **Result Handling** option to write the source code file to disk and look up what exactly PRTG gets when calling the URL. If the URL configured does not point to a web page, but to a binary file, for example, to an image, you usually will not check for content.

AUTHENTICATION

Authentication	Define if the web page at the configured URL needs authentication. Choose between: <ul style="list-style-type: none"> ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between: <ul style="list-style-type: none"> ▪ Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. <ul style="list-style-type: none">  This authentication method transmits credentials as plain text. ▪ Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.

AUTHENTICATION

- **Digest Access Authentication:** Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication.

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http://](#) or [https://](#) or even a simple slash / as equivalent for [http://](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https://](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)
- Using the value [/help](#) in the URL field, PRTG will automatically create and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?

- <https://kb.paessler.com/en/topic/30593>

Knowledge Base: Is it possible to test a WSDL or SOAP service with PRTG?

- <https://kb.paessler.com/en/topic/66680>

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Knowledge Base: Why do my HTTP Advanced sensors differ in the bytes received value?

- <https://kb.paessler.com/en/topic/78778>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

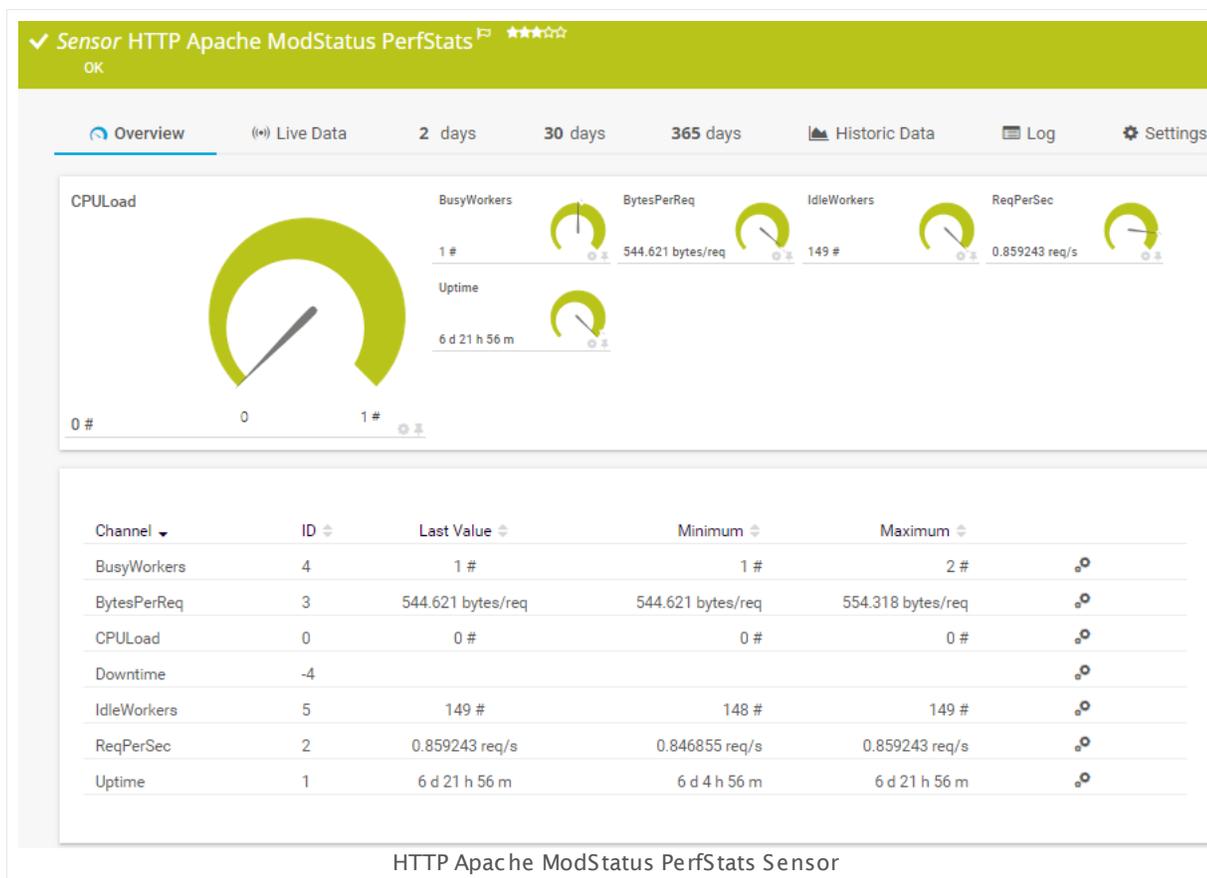
7.8.51 HTTP Apache ModStatus PerfStats Sensor

The HTTP Apache ModStatus PerfStats sensor monitors performance statistics of an Apache web server using `mod_status` over Hypertext Transfer Protocol (HTTP).

It can show the following about the Apache at scan time:

- CPU load
- Server uptime
- Requests per second
- Bytes per request
- Number of current busy worker threads
- Number of idle worker threads

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: HTTP Apache ModStatus PerfStats, French: HTTP Apache ModStatus PerfStats, German: HTTP Apache ModStatus PerfStats, Japanese: HTTP Apache ModStatus 性能統計,

Portuguese: **HTTP Apache ModStatus PerfStats**, Russian: **HTTP Apache ModStatus — стат. произв-сти**, Simplified Chinese: HTTP Apache ModStatus PerfStats, Spanish: **ModStatus PerfStats de HTTP Apache**

Remarks

- Supports [Smart URL Replacement](#)^[990].
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited ^[140] from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

URL Enter the URL to the **mod_status** module on your Apache server. PRTG will append a **/server_status?auto** part automatically. If you enter an absolute URL, this address will be independent from the **IP Address/DNS Name** setting of the device this sensor is created on.

i PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

i This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

AUTHENTICATION

Authentication Define if the web page at the configured URL needs authentication. Choose between:

- **No authentication needed**
- **Web page needs authentication**

User This field is only visible if you enable authentication above. Enter a username. Please enter a string.

AUTHENTICATION

- Password** This field is only visible if you enable authentication above. Enter a password. Please enter a string.
- Authentication Method** This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:
- **Basic access authentication (HTTP):** Use simple HTTP authentication. This is the default setting and suitable for most cases.
 This authentication method transmits credentials as plain text.
 - **Windows NT LAN Manager (NTLM):** Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
 - **Digest Access Authentication:** Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication.
- We recommend that you use the default value.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)^[338].
-  The [SSL Certificate Sensor](#)^[2635] and the [SSL Security Check Sensor](#)^[2646] do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

 Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http://](#) or [https://](#) or even a simple slash [/](#) as equivalent for [http://](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** `www.example.com` and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value `https:///` in the URL field, PRTG will automatically create the URL `https://www.example.com/`
- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL `http://www.example.com/help`
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, `http://:8080/`

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

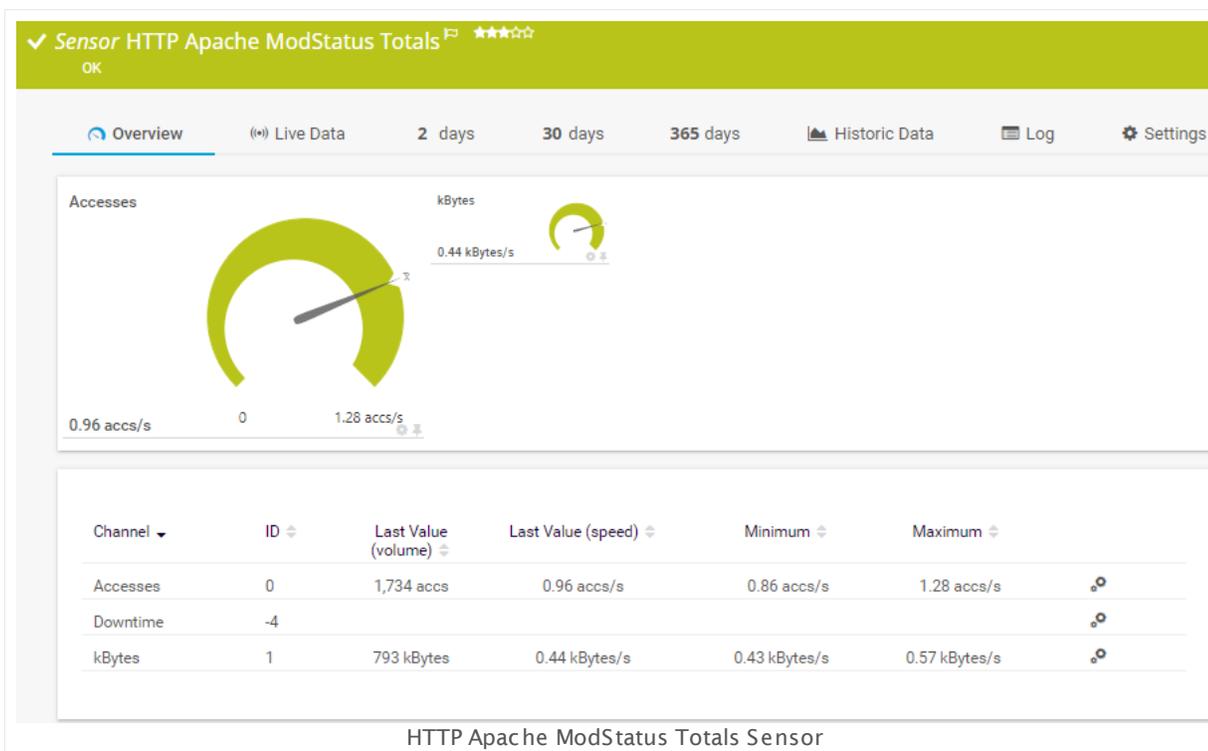
7.8.52 HTTP Apache ModStatus Totals Sensor

The HTTP Apache ModStatus Totals sensor monitors the activity of an Apache web server using `mod_status` over Hypertext Transfer Protocol (HTTP).

It can show the following:

- Number of accesses
- Transferred data in kilobytes per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **HTTP Apache ModStatus Totalen**, French: **Totaux HTTP Apache ModStatus**, German: **HTTP Apache ModStatus Totals**, Japanese: **HTTP Apache ModStatus 合計**, Portuguese: **HTTP Apache ModStatus totais**, Russian: **HTTP Apache ModStatus — итоги**, Simplified Chinese: **HTTP Apache ModStatus ? ?**, Spanish: **ModStat us total de HTTP Apache**

Remarks

- Supports [Smart URL Replacement](#) ¹⁰⁰⁰.
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
URL	<p>Enter the URL to the mod_status module on your Apache server. PRTG will append a /server_status?auto part automatically. If you enter an absolute URL, this address will be independent from the IP Address/DNS Name setting of the device this sensor is created on.</p> <p> PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section Smart URL Replacement below.</p>

-  This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

AUTHENTICATION

Authentication	<p>Define if the web page at the configured URL needs authentication. Choose between:</p> <ul style="list-style-type: none"> ▪ No authentication needed ▪ Web page needs authentication
User	This field is only visible if you enable authentication above. Enter a username. Please enter a string.
Password	This field is only visible if you enable authentication above. Enter a password. Please enter a string.
Authentication Method	<p>This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:</p> <ul style="list-style-type: none"> ▪ Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases. ▪  This authentication method transmits credentials as plain text.

AUTHENTICATION

- **Windows NT LAN Manager (NTLM):** Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
- **Digest Access Authentication:** Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication.

We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

 This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)^[3368].

 The [SSL Certificate Sensor](#)^[2635] and the [SSL Security Check Sensor](#)^[2646] do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

 Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

 Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[3355] on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)

- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

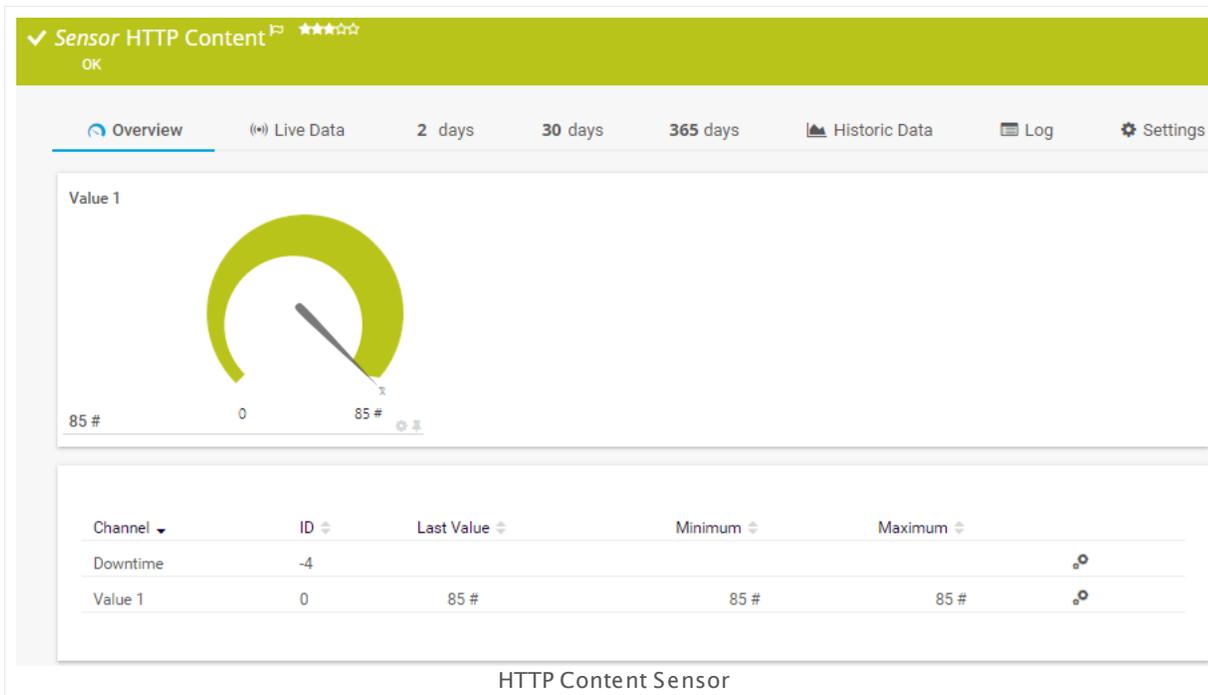
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.53 HTTP Content Sensor

The HTTP Content sensor monitors a numerical value returned by an Hypertext Transfer Protocol (HTTP) request. In the returned HTML page, each value must be placed between square brackets []. See the [example](#) below.

- It shows the returned numbers in dedicated channels, one channel for each value.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **HTTP (Inhoud)**, French: **HTTP (contenu)**, German: **HTTP (Inhalt)**, Japanese: **HTTP コンテンツ**, Portuguese: **Conteúdo HTTP**, Russian: **HTTP: Содержимое**, Simplified Chinese: **HTTP ? ?**, Spanish: **HTTP Contenido**

Remarks

- This sensor [does not support more than 50 channels](#) officially.
- Supports [Smart URL Replacement](#).
- Knowledge Base: [How can I monitor internal values of a web application with PRTG?](#)
- See also the PRTG manual: [HTTP Content Sensor—Example](#)
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP SPECIFIC

Value Type	<p>Define what kind of values your HTML file gives back. Choose between:</p> <ul style="list-style-type: none"> ▪ Integer: An integer is expected as return value. ▪ Float: A float is expected as return value, with a dot <code>.</code> between pre-decimal position and decimal places. In this setting, the sensor will also display integer values unless they don't produce a buffer overflow. <p> The sensor cannot handle string values.</p>
Number of Channels	<p>Define how many values your HTML file gives back. The sensor handles each value in its own sensor channel^[136]. Each value must be placed between square brackets <code>[]</code>. Enter the number of bracket-value pairs that the defined URL will return. Please enter an integer value.</p> <p> Do not enter a number less than the number of values returned. Otherwise you will get an error message.</p>

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Script URL	<p>Enter the URL the sensor connects to. It has to be URL encoded! If you enter an absolute URL, this address will be independent from the IP Address/DNS Name setting of the device this sensor is created on.</p> <p>i PRTG uses a smart URL replacement that allows you to use the parent device's IP Address/DNS Name setting as part of the URL. For more information, see section Smart URL Replacement below.</p>

HTTP SPECIFIC

Value Type	Shows the kind of values that the HTML file returns. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------------	---

-  This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

Content Changes Define what the sensor will do if the content of the monitored web page changes. Choose between:

- **Ignore changes:** No action will be taken on change.
- **Trigger 'change' notification:** The sensor will send an internal message indicating that the web page content has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³¹⁷⁰ whenever the web page content changes.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

AUTHENTICATION

Authentication	<p>Define if the web page at the configured URL needs authentication. Choose between:</p> <ul style="list-style-type: none">▪ No authentication needed▪ Web page needs authentication
User	<p>This field is only visible if you enable authentication above. Enter a username. Please enter a string.</p>
Password	<p>This field is only visible if you enable authentication above. Enter a password. Please enter a string.</p>
Authentication Method	<p>This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:</p> <ul style="list-style-type: none">▪ Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases.  This authentication method transmits credentials as plain text.▪ Windows NT LAN Manager (NTLM): Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.▪ Digest Access Authentication: Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication. <p>We recommend that you use the default value.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷¹ group's settings, see section [Inheritance of Settings](#)¹³⁷¹ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷¹ for more information.

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

i This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.

i The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name

Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port

Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

PROXY SETTINGS FOR HTTP SENSORS

User	<p>If the proxy requires authentication, enter the username for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>
Password	<p>If the proxy requires authentication, enter the password for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[335] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Example

- For example, consider a URL <http://www.example.com/status.html> that returns a PHP script with the current system status in a simple HTML page as follows:

```
<html>
<body>
  Description: Script gives back current status of disk free (%) and CPU usage (%).
  [85.5][12.0]
</body>
</html>
```

You would configure the HTTP Content sensor using

- the script **URL** from above,
- value type **Float**,
- and number of channels **2**.

The sensor calls the URL with every scanning interval and only regard the two values in square brackets `[]`, handling each of them in one sensor channel. The additional description text and HTML tags are not necessary. In this example they are added in case a human calls the URL.

i If you define the number of channels as **1**, the sensor will read only the first value. The second value will be ignored. Using **3** as number of channels will result in a sensor error message.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either <http://> or <https://> or even a simple slash `/` as equivalent for <http://>). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** www.example.com and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value <https://> in the URL field, PRTG will automatically create the URL <https://www.example.com/>
- Using the value [/help](http://www.example.com/help) in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: How can I monitor internal values of a web application with PRTG?

- <https://kb.paessler.com/en/topic/4>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

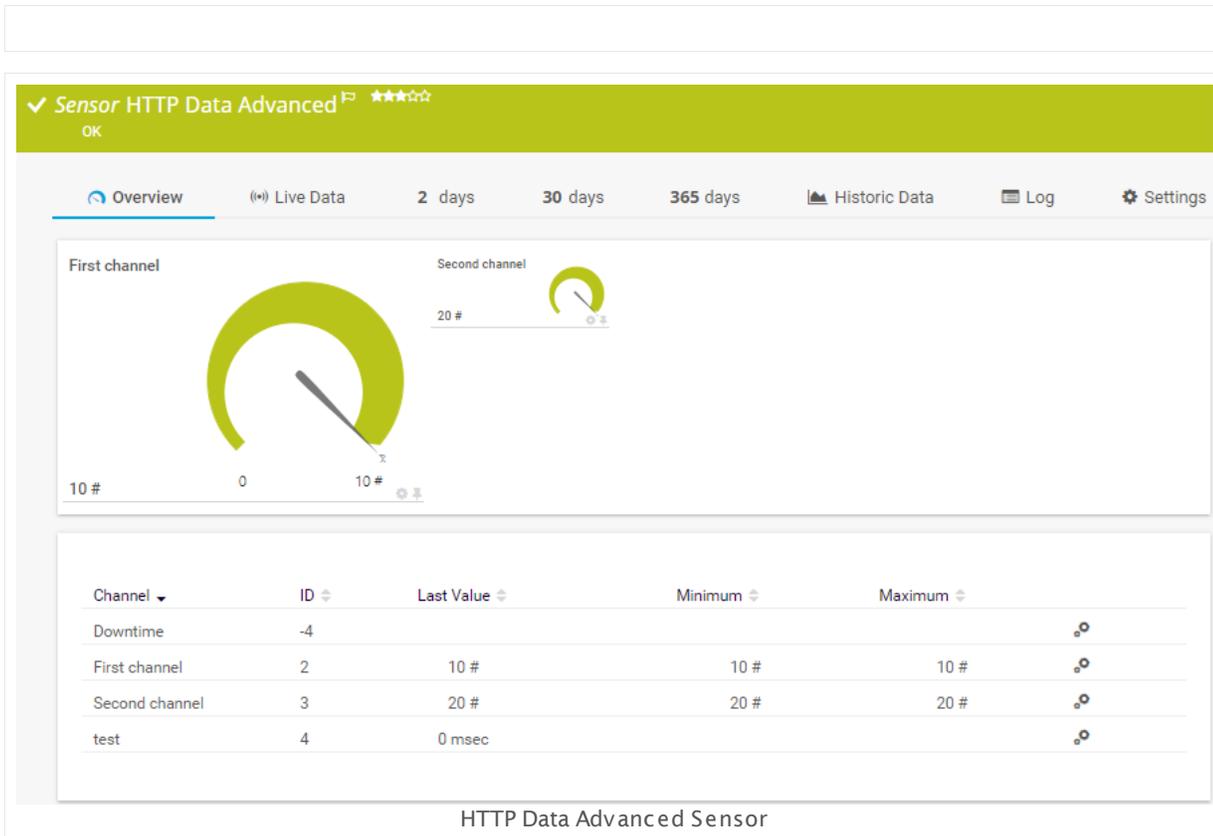
For more general information about settings, see the [Object Settings](#)²¹⁷¹ section.

7.8.54 HTTP Data Advanced Sensor

The HTTP Data Advanced sensor accesses a web server and retrieves XML or JSON encoded data.

- The sensor can show values returned by the web server in multiple channels.

For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.



Sensor in Other Languages

Dutch: **HTTP Data Geavanceerd**, French: **Données avancées HTTP**, German: **HTTP Daten (Erweitert)**, Japanese: **HTTP データアドバンスド**, Portuguese: **Dados HTTP Avançado**, Russian: **HTTP: Данные (Расширенный)**, Simplified Chinese: **HTTP ? ? ? ?**, Spanish: **Datos HTTP avanzados**

Remarks

- The requested web server must return XML or JSON encoded data that matches the format as defined in manual section [Custom Sensors](#)³⁶⁴¹.
- For best sensor performance, we recommend you specify the content type on the target server, which is `application/xml` or `application/json`.
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

URL Enter the URL the sensor connects to. It has to be **URL encoded!**

If you enter an absolute URL, the sensor uses this address independently from the **IP Address/DNS Name** setting of the device on which you create this sensor. You can enter an URL leading to a webpage (to measure the page source code's loading time), or enter the URL of an image or of another page asset to measure this element's availability and loading time.

 PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Request Method Choose an HTTP request method to determine how the sensor will request the given URL.

- **GET:** Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST:** Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Postdata** field below.
- **HEAD:** Only request the HTTP header from the server without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata This field is only visible when you select the **POST Request Method** setting above. Enter the data part for the POST request here.

 No XML is allowed here!

Content Type This setting is only visible when you select the **POST Request Method** setting above. Define the content type of a POST request. Choose between:

- **Default (application/x-www-form-urlencoded):** This is the default content type used to encode the form data set for submission to the server.
- **Custom:** If you need another content type than default, enter this content type below.

HTTP SPECIFIC

- Custom Content Type** This field is only visible when you select **Custom** above. Define the content type that is needed, for example, XML, JSON, HTTP.
- Server Name Indication** Shows the Server Name Identification (SNI) that the sensor automatically determined from the host address of the [parent device](#)^[402] or the target URL of the sensor. SNI has to be a **Fully Qualified Domain Name (FQDN)**. Please ensure it matches the configuration of the target server.
-  For details, see the Knowledge Base article [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)
- SNI Inheritance** Define if you want to inherit the Server Name Identification (SNI) from the parent device. See the **Server Name Indication** setting above which SNI is determined. Choose between:
- **Inherit SNI from parent device:** The sensor determines the SNI from the host address of the parent device.
 - **Do not inherit SNI from parent device:** The sensor determines the SNI from the target **URL** as defined in the settings of this sensor.

- Result Handling** Define what the sensor will do with the data loaded at the given URL. Choose between:
- **Discard HTML result:** Do not store the requested data.
 - **Store latest HTML result:** Store the last result of the requested data to the **Logs (Sensors)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: **Result of Sensor [ID].txt**. This is for debugging purposes, especially in combination with content checks. The file will be overridden with each scanning interval.
-  For information on how to find the folder used for storage, see section [Data Storage](#)^[3734].
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

ADVANCED SENSOR DATA

Protocol Version	<p>Define the HTTP protocol version that the sensor will use when connecting to the target URL. Choose between:</p> <ul style="list-style-type: none">▪ HTTP 1.0▪ HTTP 1.1: This is the default setting.
User Agent	<p>Choose which user agent string the sensor will send when connecting to the target URL. Choose between:</p> <ul style="list-style-type: none">▪ Use PRTG's default string: Do not enter a specific user agent, use the default setting. Usually, this is: Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)▪ Use a custom string: Use a custom user agent. Define below.
Custom User Agent	<p>This field is only visible if you enable custom user agent above. Enter a string to be used as user agent when connecting to the URL specified above.</p>
Use Custom HTTP Headers	<p>Define if you want to send custom HTTP headers to the target URL. Choose between:</p> <ul style="list-style-type: none">▪ Do not use custom HTTP headers▪ Use custom HTTP headers
Custom HTTP Headers	<p>This field is only available if you select using custom headers above. Enter a list of custom HTTP headers with their respective values that you want to transmit to the URL you define above, each pair in one line. The syntax of a header-value pair is header1:value1</p> <p> The sensor does not support the header field names user-agent, content-length, host.</p> <p> Ensure the HTTP header statement is valid! Otherwise, the sensor request will not be successful.</p>

AUTHENTICATION

Authentication	<p>Define if the web page at the configured URL needs authentication. Choose between:</p> <ul style="list-style-type: none">▪ No authentication needed▪ Web page needs authentication
----------------	--

AUTHENTICATION

- User** This field is only visible if you enable authentication above. Enter a username. Please enter a string.
- Password** This field is only visible if you enable authentication above. Enter a password. Please enter a string.
- Authentication Method** This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:
- **Basic access authentication (HTTP):** Use simple HTTP authentication. This is the default setting and suitable for most cases.
 This authentication method transmits credentials as plain text.
 - **Windows NT LAN Manager (NTLM):** Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
 - **Digest Access Authentication:** Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication.
- We recommend that you use the default value.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷¹ group's settings, see section [Inheritance of Settings](#)¹³⁷¹ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷¹ for more information.

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

- ⓘ This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
- ⓘ The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name

Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port

Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

PROXY SETTINGS FOR HTTP SENSORS

User	<p>If the proxy requires authentication, enter the username for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>
Password	<p>If the proxy requires authentication, enter the password for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[335] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)
- Using the value [/help](#) in the URL field, PRTG will automatically create and monitor the URL [http://www.example.com/help](#)
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, [http://:8080/](#)

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

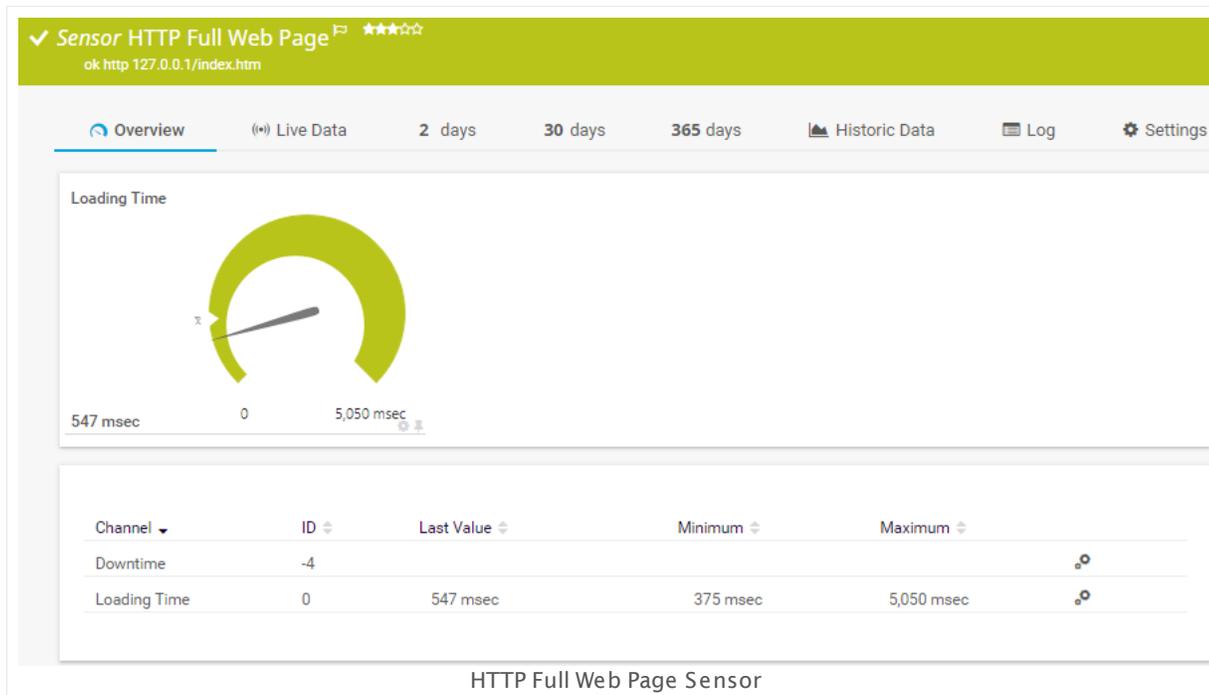
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.55 HTTP Full Web Page Sensor

The HTTP Full Web Page sensor monitors the full download time of a web page including assets such as images. In the background, it opens the web page in a browser instance to perform the measurement. Links are not followed.

- This sensor shows the loading time of the full web page.

⚠ Be careful with this sensor, because it can generate considerable internet traffic if you use it with a low scanning interval!



Sensor in Other Languages

Dutch: **HTTP Volledige Webpagina**, French: **HTTP (page Web complète)**, German: **HTTP (Komplette Webseite)**, Japanese: **HTTP 完全 Web ページ監視**, Portuguese: **HTTP Página Completa**, Russian: **HTTP: Полное время загрузки веб-страницы**, Simplified Chinese: **HTTP ? ? ? ?**, Spanish: **HTTP Página Web Completa**

Remarks

- Supports [Smart URL Replacement](#)
- Knowledge Base: [What to do when I see a CreateUniqueTempDir\(\) error message for my HTTP Full Webpage Sensor?](#)
- Knowledge Base: [HTTP Full Web Page sensor is unable to navigate. What can I do?](#)
- Knowledge Base: [How can I change the size of PhantomJS full web page screenshots?](#)
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

FULL PAGE DOWNLOAD SETTINGS

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

URL Enter the address of the web page that the sensor loads. It has to be **URL encoded!** If you enter an absolute URL, this address will be independent from the **IP Address/DNS Name** setting of the device this sensor is created on.

PRTG uses a smart URL replacement that allows you to use the parent device's **IP Address/DNS Name** setting as part of the URL. For more information, please see section **Smart URL Replacement** below.

Browser Engine Define which browser the sensor uses to load the web page. Choose between:

- **Chromium (recommended):** Use the "WebKit" engine that is delivered with PRTG to perform the loading test. With each scanning interval, PRTG will load the URL defined above in an instance of "Chromium" and measure the time until the page is fully loaded. This is the recommended setting.
- **PhantomJS (Headless Webkit):** Use the "PhantomJS" engine. This engine can have a high impact on your probe system's CPU and memory load, but there are additional options for result handling available (see below).
- **Internet Explorer:** With each scanning interval, the URL defined above is loaded in the background in an instance of Internet Explorer. PRTG uses the Internet Explorer of the system running the PRTG probe.
 For full functionality we strongly recommend you to install Internet Explorer 11 or higher on the system running the PRTG probe. The probe machine is either the local system (on every node, if on a cluster probe), or the system running the [remote probe](#)³⁷⁰⁹ where the sensor is created.

FULL PAGE DOWNLOAD SETTINGS

 For all browser engines, the same proxy settings are used that are configured for the Windows user account that the PRTG probe is running on (this is usually the Windows local "system" user account, if not changed). These settings are accessible via the Internet Explorer of this system. If you want to use a proxy for this full web page sensor test, for example, please adjust the Internet Explorer's settings accordingly (on the computer running the probe; on all nodes, if in a cluster).

Security Context

Define the Windows user account that the sensor uses to run the browser engine. Choose between:

- **Use security context of probe service (default):** Run the browser engine under the same Windows user account the PRTG probe is running on. By default, this is the local Windows "system" user account (if not manually changed).

- **Use Windows credentials of parent device:** Use the Windows user account defined in the settings of the parent device this sensor is created on. Open the sensor's parent [device settings](#)  to change the Windows credentials.

 We recommended that you use this setting when using the Chromium browser engine.

Result Handling

This setting is only visible if you select the PhantomJS engine above. This browser engine can render and store screenshots of the loaded web page. Choose between:

- **Discard HTML result (recommended):** Do not store the requested web page.

- **Render and store a screenshot of most recent sensor result as JPG:** Render and store the last result of the web page to the **Logs (Sensors)** directory (on the remote system, when used on a remote probe; on the Master node, if in a cluster). This is for debugging purposes. The file will be overridden with each scanning interval. It will be named using the pattern **Fullpage of Sensor (ID).jpg**.

 For information on how to find the folder used for storage, see section [Data Storage](#) .

FULL PAGE DOWNLOAD SETTINGS

- **Render and store screenshots of all sensor results as JPGs (requires lots of disk space):** Render and store one new screenshot of the web page with each sensor scan, and store the pictures in the **Screenshots (Fullpage Sensor)** directory (on the remote system, when used on a remote probe). This option can be used to create a visual history of the web page.

 For information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 Depending on the monitored website and the scanning interval of the sensor, this option can create a very high amount of data! Use with care and make sure you set appropriate data purging limits in the [System Administration—Core & Probes](#)³³⁷³ settings.

 If necessary, you can change the window size of the rendered screenshots. For details, see the Knowledge Base article [How can I change the size of PhantomJS full web page screenshots?](#)

 Depending on the result handling method you choose, the sensor does not only store files in the screenshot directory, but there will also be files in an extra cache directory. If your disk on the probe system runs full, please also check this path (you might have to set folder options appropriately to see this directory):

`C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5`

Authentication

This setting is only visible if you select the **PhantomJS** engine above. Define if the monitored web page needs authentication for access. Choose between:

- **No authentication needed:** Access to the web page is granted without authentication.
- **Web page needs authentication:** PRTG automatically tries to use HTTP Basic authentication (BA) or Windows NT LAN Manager (NTLM) to access the web page with authentication. Enter the credentials below.

 Basic access authentication forwards the credentials in plain text!

User

This setting is only visible if you select the **PhantomJS** engine with authentication above. Enter the username for the web page.

Password

This setting is only visible if you select the **PhantomJS** engine with authentication above. Enter the password for the web page.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)

- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: What to do when I see a `CreateUniqueTempDir()` error message for my HTTP Full Webpage Sensor?

- <https://kb.paessler.com/en/topic/40783>

Knowledge Base: HTTP Full Web Page sensor is "unable to navigate". What can I do?

- <https://kb.paessler.com/en/topic/59999>

Knowledge Base: How can I change the size of PhantomJS full web page screenshots?

- <https://kb.paessler.com/en/topic/60247>

Knowledge Base: What is the difference between "HTTP" and "HTTP Full Web Page" Web Server sensors?

- <https://kb.paessler.com/en/topic/943>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

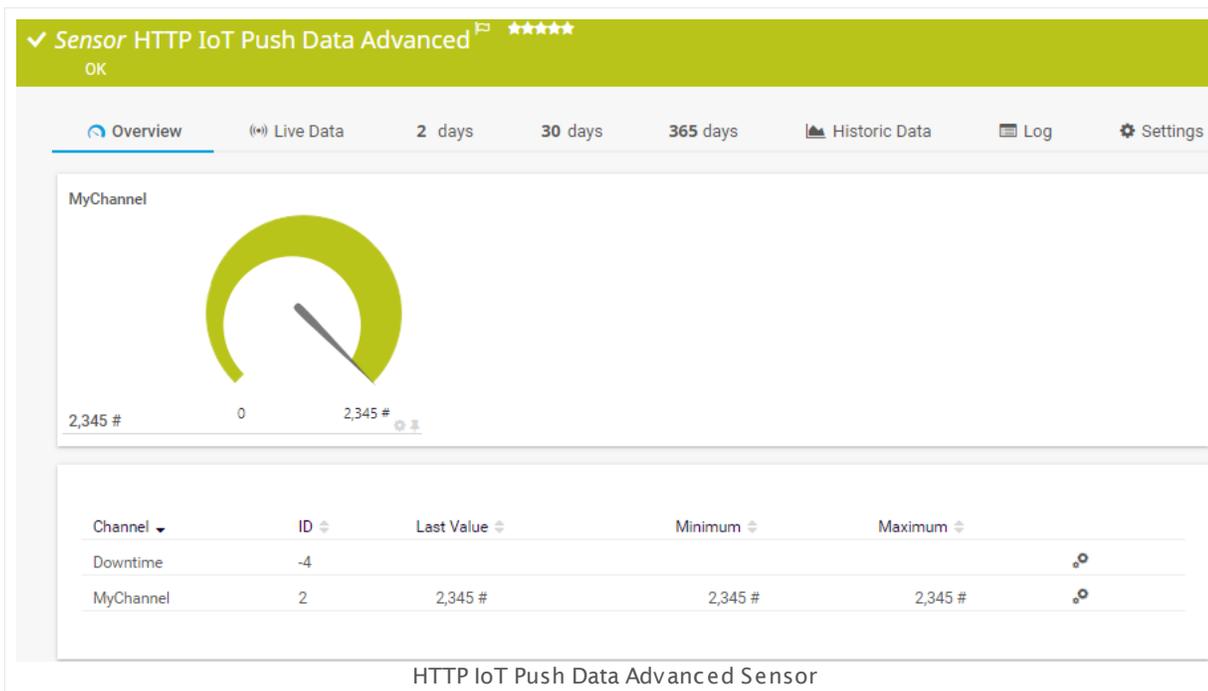
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.56 HTTP IoT Push Data Advanced

The HTTP IoT Push Data Advanced sensor displays data from messages received from IoT-capable devices (for example, Sigfox devices) that are pushed via a Hypertext Transfer Protocol Secure (HTTPS) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTPS (TLS 1.2 encrypted). This sensor type is especially useful when you want to push data to a PRTG hosted by Paessler instance.

- This sensor can show received values and a message encoded in valid XML or JSON in multiple channels.

For details about the return value format, see section [Custom Sensors](#).



Sensor in Other Languages

Dutch: **HTTP Push Data geavanceerd**, French: **Données avancées Push HTTP**, German: **HTTP Push-Daten (Erw.)**, Japanese: **HTTP プッシュデータ(アドバンスド)**, Portuguese: **Dados HTTP Avançado via Push**, Russian: **HTTP: Данные push-объекта (Расширенный)**, Simplified Chinese: **HTTP ? ? ? ? ? ? ?**, Spanish: **Datos Push de HTTP avanzandos**

Remarks

- For details about the usage, see manual section [HTTP IoT Push Data Advanced Sensor—How to Use](#).
- If you use this sensor with multiple channels, we recommend that you **simultaneously** push the data for **all** your channels to the PRTG server. You can push data to only one of your sensor channels, but in this case all other channels will record the value of **0** for this push message.

- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- This sensor type has a fixed port (5051). You cannot change it.
- This sensor type has a fixed SSL version (HTTPS (TLS 1.2 only)). You cannot change it.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
- For a general introduction to the technology behind push, please see the manual section [Monitoring via Push](#) ³⁶⁴⁰.

How to Use

This function is known as **webhook**. Basically, a webhook works like a **push notification**. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP IoT Push Data Advanced sensor then displays the data of pushed and received messages.

The data that is pushed to this sensor must be valid XML or JSON.

 For details about the return value format, see section [Custom Sensors](#) ³⁶⁴¹.

The **HTTP IoT Push Data Advanced Sensor** uses the following URLs depending on the type of HTTPS request.

- **GET requests:** `https://<probe_ip>:5051/<token>?content=<valid XML_or_JSON>`

The XML encoded value of the content parameter has to match the format as defined in section [Custom Sensors](#) ³⁶⁴¹.

- **POST requests:** `https://<probe_ip>:5051/<token>`

This HTTPS request method sends the XML or JSON encoded HTTPS body as POST data. The body has to match the format as defined in section [Custom Sensors](#) ³⁶⁴¹. We strongly recommend the HTTPS content type `application/xml` or `application/json`.

Replace the parameters `<probe_ip>`, `<token>`, and `<valid XML_or_JSON>` (for GET requests) with the corresponding values:

- For PRTG on premises, the **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running. For PRTG hosted by Paessler instances, the **probe IP** is the DNS name of the instance.
- The **port number** is always `5051`. You cannot change this.
- You can define **identification token** in the sensor settings.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
 -  The content has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Minimum example for the GET method that returns one static channel value:

```
https://127.0.0.1:5051/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10</value></result>
```

! By default, values within the `<value>` tags in the returned XML or JSON must be **integers** to be processed. If **float** values are returned, you have to explicitly define this value type as defined in section [Custom Sensors](#) with `<float>` tags, otherwise the sensor will show **0** values in affected channels. Example:

```
https://127.0.0.1:5051/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>
```

i You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSL SETTINGS

SSL Settings The security of the incoming HTTPS push requests.

- **HTTPS (TLS 1.2 only):** Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections.

This setting is shown for your information only and cannot be changed.

SSL Port The number of the port on which this sensor listens for incoming HTTPS requests. This is always **5051**.

This setting is shown for your information only and cannot be changed.

HTTP PUSH AUTHENTICATION

Identification Token This is the token that is used to find the matching sensor for the incoming message. When you create the sensor, this token is `{__guid__}`.

This token will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation.

 The token will not be replaced automatically if you change it already during sensor creation.

HTTP PUSH DATA

No Incoming Data

Define which [status](#)¹⁹⁵ the sensor will show if it has not received a push message for at least two sensor scans. Choose between:

- **Ignore and keep last status (default):** The sensor remains in the status as defined by the last message that the sensor received.
 The probe on which this sensor runs must be connected to keep the last status. If the probe is disconnected, the sensor will show the **Unknown** status. If the probe is connected again, the sensor does not automatically return from **Unknown** to the last status before the probe disconnect.
- **Switch to "Unknown" status:** The sensor will show an **Unknown** status if it has not received any message for at least two sensor scans.
- **Switch to "Error" after x minutes:** The sensor will show a **Down** status if it has not received any message within a defined time span. Define the time threshold below.

Time Threshold (Minutes)

This field is only visible if you select the error option above. Enter a time threshold in minutes. If this time elapses, the sensor will show a **Down** status if it has not received a push message within this time span.

Please enter an integer value. The maximum threshold is **1440** minutes.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷¹ group's settings, see section [Inheritance of Settings](#)¹³⁷¹ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷¹ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I monitor Sigfox Geolocation with PRTG?

- <https://kb.paessler.com/en/topic/80157>

Knowledge Base: How can I monitor the Sigfox API with PRTG?

- <https://kb.paessler.com/en/topic/80346>

Knowledge Base: How can I monitor Sigfox Callbacks with PRTG?

- <https://kb.paessler.com/en/topic/80232>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

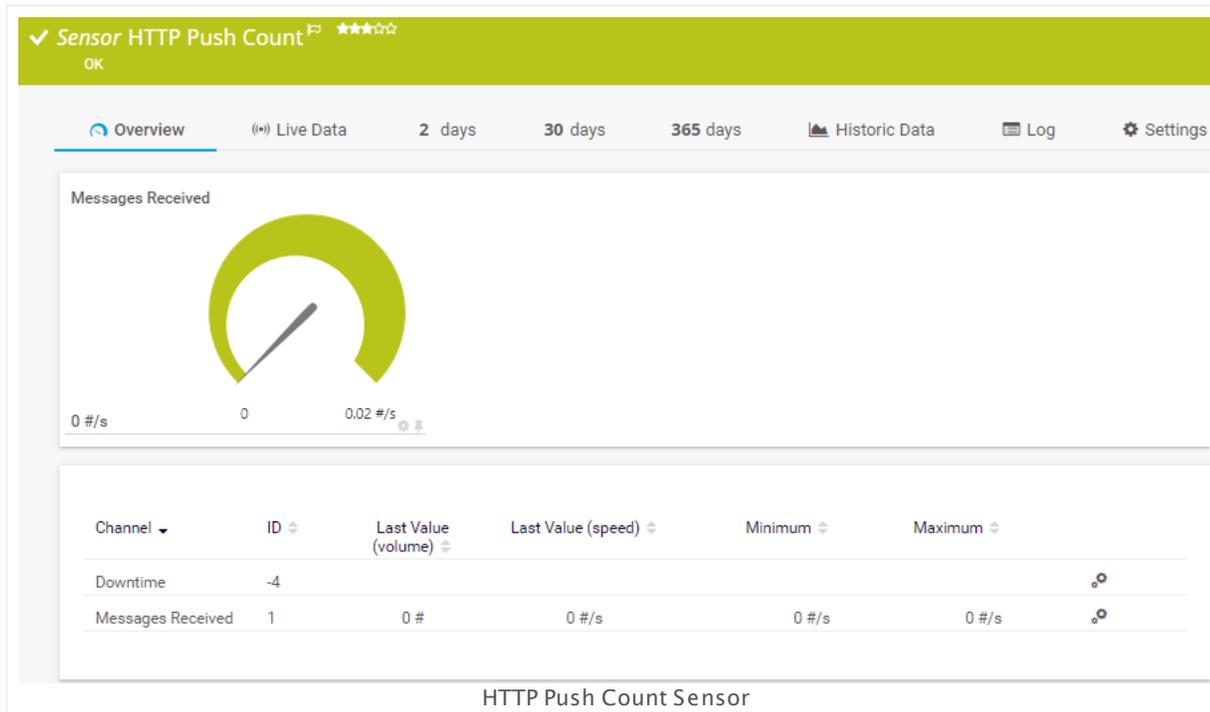
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.57 HTTP Push Count Sensor

The HTTP Push Count sensor counts received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- It shows the number of received messages per second.



Sensor in Other Languages

Dutch: **HTTP Push Aantal**, French: **Nombre de Push HTTP**, German: **HTTP Push-Anzahl**, Japanese: **HTTP プッシュ数**, Portuguese: **Contagem de push HTTP**, Russian: **HTTP: Количество push-объектов**, Simplified Chinese: **Http ? ? ?**, Spanish: **Recuento Push de HTTP**

Remarks

- For details about the usage, see manual section [HTTP Push Count Sensor—How to Use](#) ¹⁰⁵⁰.
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - For a general introduction to the technology behind push, please see the manual section [Monitoring via Push](#) ³⁵⁴⁸.
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as **webhook**. Basically, a webhook works like a **push notification**. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Count sensor then displays the number of pushed and received messages.

The **HTTP Push Count Sensor** uses the following URL:

```
http://<probe_ip>:<port_number>/<token>
```

Replace the parameters **<probe_ip>**, **<port_number>**, and **<token>** with the corresponding values.

- The **<probe_ip>** is the IP address of the system where the PRTG probe with the sensor is running.
- The **<port_number>** is where the sensor listens for incoming HTTP calls.
- The **<token>** is used to define the matching sensor.

Example:

```
http://192.0.2.0:5050/XYZ123
```

 You can use several sensors with the same port and identification token. In this case, the number of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you **manually**  add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings

Define the security of the incoming HTTP push requests. Choose between:

- **HTTP (unsafe):** Send push messages to the PRTG probe system via insecure HTTP.

HTTP PUSH

- **HTTPS (TLS 1.2 only):** Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or [your own trusted SSL certificate](#) that you have imported for the PRTG web server.

Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is 5050 .
SSL Port	This field is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is 5051 .

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP PUSH

SSL Settings Shows whether the sensor accepts push messages via HTTP or HTTPS.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Port This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSL Port This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Request Method Select the request method of your webhook:

- **ANY:** Do not use any filter for the request method.
- **GET:** Choose this method if your webhook uses GET.
- **POST:** Choose this method if your webhook sends post form data. Postdata has to be `application/x-www-form-urlencoded` with the same parameters as for GET requests.

HTTP PUSH

- Identification Token** This is the token that is used to find the matching sensor for the incoming message. When you create the sensor, this token is `{_guid_}`.
- This token will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation.
-  The token will not be replaced automatically if you change it already during sensor creation.
- Incoming Request** Define what PRTG will do with the incoming messages. Choose between:
- **Discard request:** Do not store the pushed messages.
 - **Write request to disk (Filename: "Request for Sensor [ID].txt"):** Store the last message received from the sensor to the **Logs (Sensor)** directory (on the Master node, if in a cluster). File name: `Request for Sensor [ID].txt`. This is for debugging purposes. The file will be overridden with each scanning interval.
 -  For information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

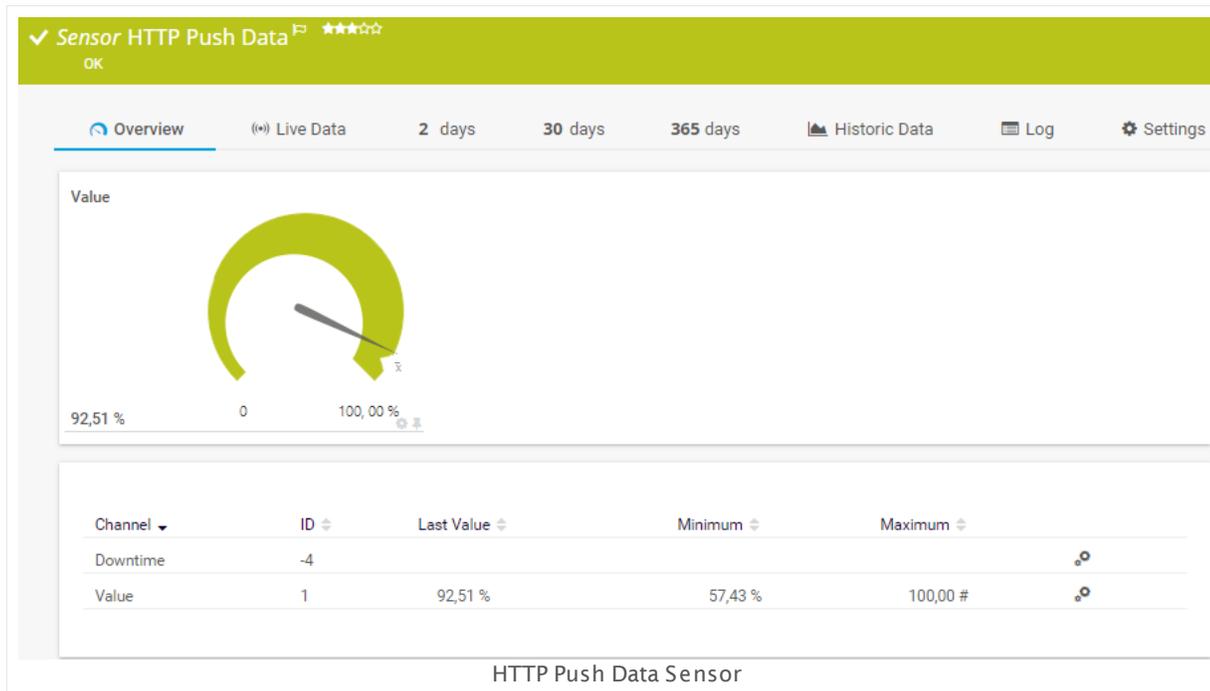
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.58 HTTP Push Data Sensor

The HTTP Push Data sensor displays numerical values from received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- The sensor shows the received value and an optional message in one channel.



Sensor in Other Languages

Dutch: **HTTP Push Data**, French: **Données Push HTTP**, German: **HTTP Push-Daten**, Japanese: **HTTP プッシュデータ**, Portuguese: **Dados HTTP via Push**, Russian: **HTTP: Данные push-объекта**, Simplified Chinese: **HTTP ? ? ? ?**, Spanish: **Datos Push de HTTP**

Remarks

- For details about the usage, see manual section [HTTP Push Data Sensor—How to Use](#).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
 - For a general introduction to the technology behind push, please see the manual section [Monitoring via Push](#).
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as **webhook**. Basically, a webhook works like a **push notification**. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Data sensor then displays the data of pushed and received messages.

The **HTTP Push Data Sensor** uses the following URL:

```
http://<probe_ip>:<port_number>/<token>?value=<integer_or_float>&text=<text message>
```

Replace the parameters **<probe_ip>**, **<port_number>**, **<token>**, and **<integer_or_float>** with the corresponding values. The **&text** parameter is optional: You can omit it.

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running.
- The **value** can be an integer or a float value, depending on the data of your application; you have to set the value type accordingly in the sensor settings. This parameter will be the sensor value.

 If this parameter is missing, the sensor will show a **down** status.

- You can **optionally** add a custom text message by replacing the parameter **<text message>** with it. The text will be shown as sensor message. If there is no value but only a text, the text will be shown as error message.

 This text message has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Example:

```
http://192.0.2.0:5050/XYZ123?value=0&text=this%20is%20a%20message
```

- ① You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you **manually**  add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings	<p>Define the security of the incoming HTTP push requests. Choose between:</p> <ul style="list-style-type: none"> ▪ HTTP (unsafe): Send push messages to the PRTG probe system via insecure HTTP. ▪ HTTPS (TLS 1.2 only): Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or your own trusted SSL certificate that you have imported for the PRTG web server.
Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is 5050 .
SSL Port	This field is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is 5051 .

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

HTTP PUSH

SSL Settings	<p>Shows whether the sensor accepts push messages via HTTP or HTTPS.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Port	<p>This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
SSL Port	<p>This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Request Method	<p>Select the request method of your webhook:</p>

HTTP PUSH

- **ANY:** Do not use any filter for the request method.
- **GET:** Choose this method if your webhook uses GET.
- **POST:** Choose this method if your webhook sends post form data. Postdata has to be **application/x-www-form-urlencoded** with the same parameters as for GET requests.

Identification Token

This is the token that is used to find the matching sensor for the incoming message. When you create the sensor, this token is **{_guid_}**.

This token will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation.

-  The token will not be replaced automatically if you change it already during sensor creation.

Incoming Request

Define what PRTG will do with the incoming messages. Choose between:

- **Discard request:** Do not store the pushed messages.
- **Write request to disk (Filename: "Request for Sensor [ID].txt"):** Store the last message received from the sensor to the **Logs (Sensor)** directory (on the Master node, if in a cluster). File name: **Request for Sensor [ID].txt**. This is for debugging purposes. The file will be overridden with each scanning interval.
 -  For information on how to find the folder used for storage, see section [Data Storage](#) 3734.

HTTP PUSH DATA

No Incoming Data

Define which [status](#)¹⁹⁵ the sensor will attain if no push message has been received for at least two sensor scans. Choose between:

- **Ignore and keep last status (default):** The sensor will remain in the status as defined by the last message received.
 - ⓘ The probe on which this sensor runs must be connected to keep the last status. If the probe is disconnected, the sensor will show the **Unknown** status. If the probe is connected again, the sensor does not automatically return from **Unknown** to the last status before the probe disconnect.
- **Switch to "Unknown" status:** The sensor will show an **Unknown** status if it has not received any message for at least two sensor scans.
- **Switch to "Error" after x minutes:** The sensor will show a **Down** status if it has not received any message within a defined time span. Define the time threshold below.

Time Threshold (Minutes)

This field is only visible if you select the error option above. Enter the time threshold in minutes after which the sensor status will show a **Down** status if it has not received a push message within this time span.

Please enter an integer value. The maximum threshold is **1440** minutes.

Value Type

Define which type the value of the received data has. If this setting does not match, the sensor will go into an **Down** status. Choose between:

- **Integer**
- **Float** (with dot . as delimiter)

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[338] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

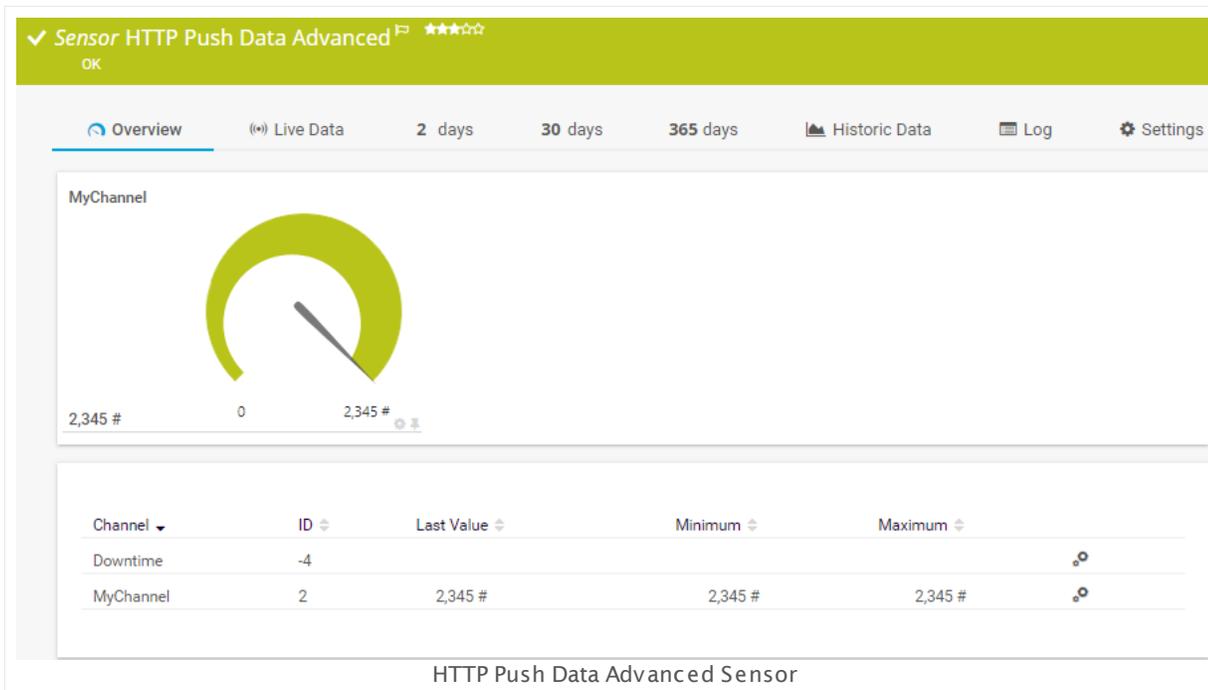
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.59 HTTP Push Data Advanced Sensor

The HTTP Push Data Advanced sensor displays data from received messages that are pushed via a Hypertext Transfer Protocol (HTTP) request to PRTG. It provides a URL that you can use to push messages to the PRTG probe system via HTTP (insecure or TLS 1.2 encrypted).

- This sensor can show received values and a message encoded in valid XML or JSON in multiple channels.

For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.



Sensor in Other Languages

Dutch: **HTTP Push Data geavanceerd**, French: **Données avancées Push HTTP**, German: **HTTP Push-Daten (Erweitert)**, Japanese: **HTTP プッシュデータ(アドバンスト)**, Portuguese: **Dados HTTP Avançado via Push**, Russian: **HTTP: Данные push-объекта (Расширенный)**, Simplified Chinese: **HTTP** ? ? ? ? ? ? , Spanish: **Datos Push de HTTP avanzandos**

Remarks

- For details about the usage, see manual section [HTTP Push Data Advanced Sensor—How to Use](#)¹⁰⁷¹.
- If you use this sensor with multiple channels, we recommend that you **simultaneously** push the data for **all** your channels to the PRTG server. You can push data to only one of your sensor channels, but in this case all other channels will record the value of **0** for this push message.
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

- For a general introduction to the technology behind push, please see the manual section [Monitoring via Push](#)³⁶⁴⁰.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

How to Use

This function is known as **webhook**. Basically, a webhook works like a **push notification**. Webhooks are usually triggered by some event (for example, a new comment to a blog post) and send according information to a specified URL. The HTTP Push Data Advanced sensor then displays the data of pushed and received messages.

The data that is pushed to this sensor must be valid XML or JSON.

 For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.

The **HTTP Push Data Advanced Sensor** uses the following URLs depending on the type of HTTP request.

- **GET** requests: `http://<probe_ip>:<port_number>/<token>?content=<valid XML_or_JSON>`

The XML encoded value of the content parameter has to match the format as defined in section [Custom Sensors](#)³⁶⁴¹.

- **POST** requests: `http://<probe_ip>:<port_number>/<token>`

This HTTP request method sends the XML or JSON encoded HTTP body as POST data. The body has to match the format as defined in section [Custom Sensors](#)³⁶⁴¹. We strongly recommend the HTTP content type `application/xml` or `application/json`.

Replace the parameters `<probe_ip>`, `<port_number>`, `<token>`, and `<valid XML_or_JSON>` (for GET requests) with the corresponding values:

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
 -  The content has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Minimum example for the GET method that returns one static channel value:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10</value></result><
```

 By default, values within the `<value>` tags in the returned XML or JSON must be **integers** to be processed. If **float** values are returned, you have to explicitly define this value type as defined in section [Custom Sensors](#)³⁶⁴² with `<float>` tags, otherwise the sensor will show **0** values in affected channels. Example:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>
```

- i** You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HTTP PUSH

SSL Settings	Define the security of the incoming HTTP push requests. Choose between: <ul style="list-style-type: none">▪ HTTP (unsafe): Send push messages to the PRTG probe system via insecure HTTP.▪ HTTPS (TLS 1.2 only): Send push messages to the PRTG probe system via secure HTTPS. The sensor only supports TLS 1.2 connections. It will use the SSL certificate that is delivered with PRTG or your own trusted SSL certificate^[3736] that you have imported for the PRTG web server.
Port	This field is only visible if you choose HTTP above. Enter the number of the port on which this sensor listens for incoming HTTP requests. Default is 5050 .
SSL Port	This field is only visible if you choose HTTPS above. Enter the number of the port on which this sensor listens for incoming HTTPS requests. Default is 5051 .

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- i** Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP PUSH

SSL Settings	<p>Shows whether the sensor accepts push messages via HTTP or HTTPS.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Port	<p>This field is only visible for sensors that accept push messages via HTTP. It shows the port number on which this sensor listens for incoming HTTP requests.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>

HTTP PUSH

SSL Port	<p>This field is only visible for sensors that accept push messages via HTTPS. It shows the port number on which this sensor listens for incoming HTTPS requests.</p> <p>Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Request Method	<p>Select the request method of your webhook:</p> <ul style="list-style-type: none">▪ ANY: Do not use any filter for the request method.▪ GET: Choose this method if your webhook uses GET.▪ POST: Choose this method if your webhook sends post form data. Postdata has to be application/x-www-form-urlencoded with the same parameters as for GET requests.
Identification Token	<p>This is the token that is used to find the matching sensor for the incoming message. When you create the sensor, this token is {_guid_}.</p> <p>This token will be replaced with an automatically generated token after you have completed the sensor creation. If you want to use another identification token, you can edit it while or after sensor creation.</p> <p> The token will not be replaced automatically if you change it already during sensor creation.</p>
Incoming Request	<p>Define what PRTG will do with the incoming messages. Choose between:</p> <ul style="list-style-type: none">▪ Discard request: Do not store the pushed messages.▪ Write request to disk (Filename: "Request for Sensor [ID].txt"): Store the last message received from the sensor to the Logs (Sensor) directory (on the Master node, if in a cluster). File name: Request for Sensor [ID].txt. This is for debugging purposes. The file will be overridden with each scanning interval.  For information on how to find the folder used for storage, see section Data Storage³⁷³⁴.

HTTP PUSH DATA

No Incoming Data

Define which [status](#)¹⁹⁵ the sensor will show if it has not received a push message for at least two sensor scans. Choose between:

- **Ignore and keep last status (default):** The sensor remains in the status as defined by the last message that the sensor received.
 - ⓘ The probe on which this sensor runs must be connected to keep the last status. If the probe is disconnected, the sensor will show the **Unknown** status. If the probe is connected again, the sensor does not automatically return from **Unknown** to the last status before the probe disconnect.
- **Switch to "Unknown" status:** The sensor will show an **Unknown** status if it has not received any message for at least two sensor scans.
- **Switch to "Error" after x minutes:** The sensor will show a **Down** status if it has not received any message within a defined time span. Define the time threshold below.

Time Threshold (Minutes)

This field is only visible if you select the error option above. Enter a time threshold in minutes. If this time elapses, the sensor will show a **Down** status if it has not received a push message within this time span.

Please enter an integer value. The maximum threshold is **1440** minutes.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- ⓘ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

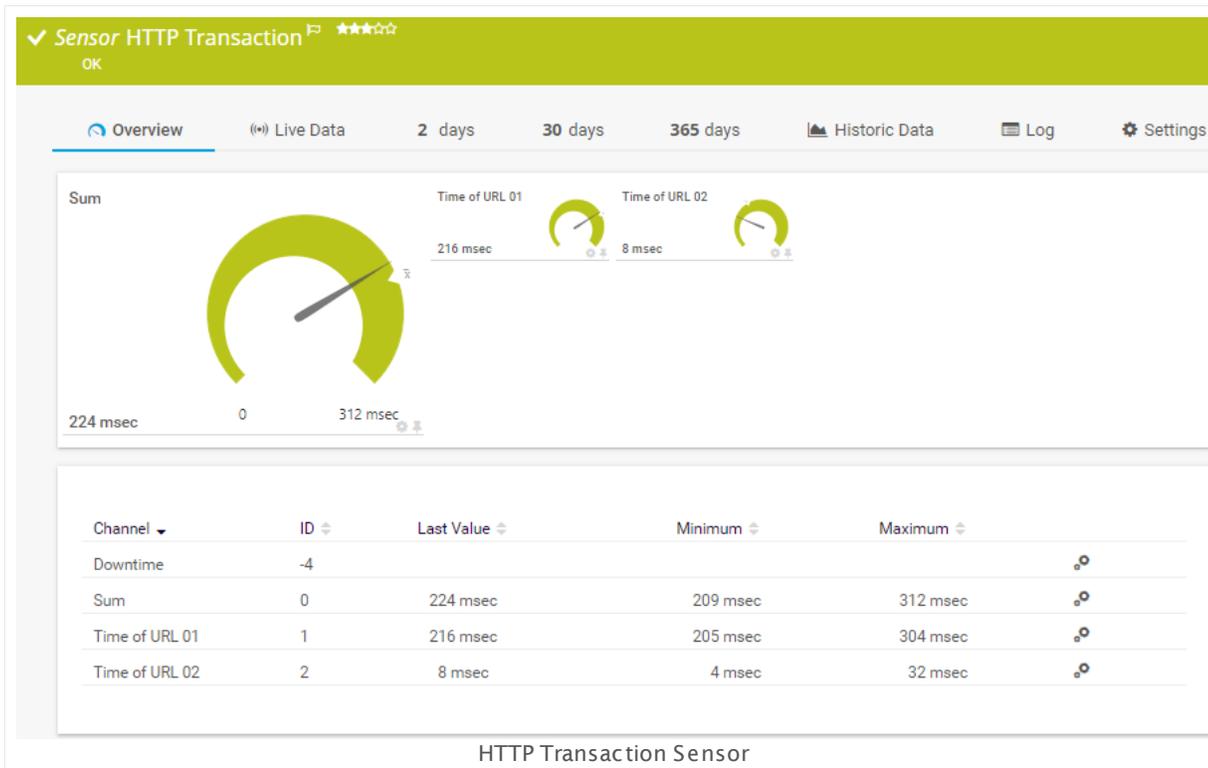
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.60 HTTP Transaction Sensor

The HTTP Transaction sensor monitors an interactive website, such as a web shop, by performing a transaction using a set of Hypertext Transfer Protocol (HTTP) URLs. The sensor monitors whether logins or shopping carts work properly.

- It shows the loading time of single URLs and of the complete transaction.



Sensor in Other Languages

Dutch: **HTTP (Transactie)**, French: **Transaction HTTP**, German: **HTTP (Transaktion)**, Japanese: **HTTP トランザクション**, Portuguese: **Transação HTTP**, Russian: **Транзакция HTTP**, Simplified Chinese: **HTTP ? ?**, Spanish: **HTTP Transacción**

Remarks

- Supports [Smart URL Replacement](#)
- Knowledge Base: [Configuration Tips for HTTP Transaction Sensors](#)
- Knowledge Base: [Which user agent should I use in the HTTP Advanced sensor's settings?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- If you need to use SRP ciphers, choose the **Alternate/ Compatibility Mode** in the sensor settings.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HTTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for all HTTP requests. If the complete transaction takes longer than this value defines, the sensor cancels the request and shows an according error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Single URL Timeout (Sec.)	Enter a timeout in seconds for one single HTTP request. If the reply of any single request takes longer than this value defines, the sensor cancels the transaction and shows an according error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

HTTP ENGINE

Monitoring Engine	<p>If you encounter unexpected errors with the standard method that is used to monitor a URL, try to use the compatibility mode, which is based on .NET. Choose between:</p> <ul style="list-style-type: none">▪ Default/High Performance (recommended): This is the default monitoring method for this sensor type.▪ Alternate/Compatibility Mode: Try this method as an alternative for websites that do not work with the default approach. Using the compatibility mode, this sensor executes an external exe. Because of this, this method needs more resources, but it can be helpful in particular cases.<ul style="list-style-type: none">❗ If you select the compatibility mode, the options for the SSL method will be slightly different. You can also check for trusted certificates. Please see below.⚠ When using the Compatibility Mode, Smart URL Replacement will not work, so this sensor will not use the IP Address/DNS value of the parent device automatically then.
-------------------	---

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

SSL Method	<p>When using the compatibility mode, the SSL specific settings are a bit different to the default (automatically used) SSL settings. You can choose between:</p> <ul style="list-style-type: none">▪ SSL 3.0▪ TLS 1.0, TLS 1.1, TLS 1.2
------------	---

SSL SPECIFIC (WHEN USING COMPATIBILITY MODE)

- **SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2** This is the default setting.
- Check SSL Certificates Specify if the sensor will check the certificate of the monitored URL. Choose between:
- **Do not check used certificates:** Do not consider the certificates of the monitored web pages. This the default setting.
 - **Check if the used certificates are trusted:** Inspect the certificates. If the certificate of the server is not trusted, the sensor shows a **Down** status and displays a corresponding message.

 This sensor type implicitly supports Server Name Identification (SNI), an extension to the TLS protocol.

ADVANCED SENSOR DATA

- Limit Download (kb) Enter a maximum amount of data that is transferred per every single request. If you set content checks below, please be aware that the sensor can only check the content downloaded within this limit for certain search expressions.
- Cookie Management Select if cookies are used for the transaction. Choose between:
- **Use cookies (recommended):** Allow cookies to be set and read during the transaction cycle.
 - **Ignore cookies:** Do not allow cookies. Use this option if you want to test the transaction without the use of cookies.
- We recommend that you use the default value.
- User Agent Choose which user agent string the sensor sends when connecting to the defined URLs. Choose between:
- **Use PRTG's Default String:** Do not enter a specific user agent, use the default setting. Usually, this is: **Mozilla/5.0 (compatible; PRTG Network Monitor (www.paessler.com); Windows)**
 - **Use a Custom String:** Use a custom user agent. Define below.
- Custom User Agent This field is only visible if you enable the **Use a Custom String** option above. Enter a string that the sensor uses as user agent when connecting to the URL specified above.

ADVANCED SENSOR DATA

Result Handling	<p>Define what PRTG will do with the web page loaded at the given URL. Choose between:</p> <ul style="list-style-type: none">• Discard HTML result: Do not store the requested web page.• Store latest HTML result: Store the last result of the requested web page to the Logs (Sensors) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File name: Result of Sensor [ID].txt. This is for debugging purposes, especially in combination with content checks. The file will be overwritten with each scanning interval.<ul style="list-style-type: none">•  For information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
-----------------	---

AUTHENTICATION

Authentication	<p>Define if the web page at the configured URL needs authentication. Choose between:</p> <ul style="list-style-type: none">▪ No authentication needed▪ Web page needs authentication
User	<p>This field is only visible if you enable authentication above. Enter a username. Please enter a string.</p>
Password	<p>This field is only visible if you enable authentication above. Enter a password. Please enter a string.</p>
Authentication Method	<p>This field is only visible if enable authentication above. Select the authentication method the given URL is protected with. Choose between:</p> <ul style="list-style-type: none">▪ Basic access authentication (HTTP): Use simple HTTP authentication. This is the default setting and suitable for most cases.<ul style="list-style-type: none">•  This authentication method transmits credentials as plain text.

AUTHENTICATION

- **Windows NT LAN Manager (NTLM):** Use the Microsoft NTLM protocol for authentication. This is sometimes used in intranets for single sign-on.
- **Digest Access Authentication:** Use digest access authentication that applies a hash function to the password, which is safer than basic access authentication.

We recommend that you use the default value.

TRANSACTION URL

- ✘ You can define up to 10 different transaction URLs, which will all be called in a row. Only if the complete transaction can be completed, the sensor will show an **Up status**¹⁹⁵. Using this mechanism you can set up an extended monitoring with multiple URLs.

Enter settings for at least one transaction URL. You can use as many steps as needed and disable the other steps.

Transaction Step #x This setting is available for URL **#2** through **#10**. Define if you want to use this step for your transaction check. Choose between:

- **Disable step #x:** Do not use this step. Choose this option if you do not need all 10 steps for your transaction check.
- **Enable step #x:** Enable this step. Further options will be viewed, as described below.

URL Enter the URL the sensor will connect to. It has to be **URL encoded!**

If you enter an absolute URL, this address will be independent from the **IP Address/DNS Name** setting of the device this sensor is created on. PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL. For more information, see section [Smart URL Replacement](#)¹⁰⁹³ below.

Request Method The request method determines how the given URL is requested.

- **GET:** Request the website directly, like browsing the web. We recommend using this setting for a simple check of a web page.
- **POST:** Send post form data to the URL. If this setting is chosen, you must enter the data that will be sent in the **Post data** field below.

TRANSACTION URL

- **HEAD:** Only request the HTTP header from the server; without the actual web page. Although this saves bandwidth since less data is transferred, it is not recommended because the measured request time is not the one experienced by your users and you might not be notified for slow results or timeouts.

Postdata

This field is only active if you choose **POST** in the **Request Method** setting above. Enter the data part for the post request here.

 No XML is allowed here!

Check For Existing Key Words (Positive)

Define whether the result at the configured URL will be checked for keywords. Choose between:

- **Disable:** Do not search for keywords.
- **Enable key word check (positive):** In the result returned at the URL, check if a key word exists.

 The content check is only intended for HTML websites and might not work with other target URLs.

Response Must Include

Define which string must be part of the web at the given URL. If the data does not include this string, the sensor will show an error status and display this string along with the affected URL in the sensor message. Please enter a string.

 Only simple text search is available here. The characters ***** and **?** work here as placeholder, whereas ***** stands for no or any number of characters and **?** stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.

Check For Existing Key Words (Negative)

Define whether the the result at the configured URL will be checked for keywords. Choose between:

- **Disable:** Do not search for keywords.
- **Enable key word check (negative):** In the result returned at the URL, check if a key word does not exist.

 The content check is only intended for HTML websites and might not work with other target URLs.

Response Must Not Include

Define which string must not be part of the web at the given URL. If the data does include this string, the sensor will show an error status and display this string along with the affected URL in the sensor message. Please enter a string.

TRANSACTION URL

 Only simple text search is available here. The characters `*` and `?` work here as placeholder, whereas `*` stands for no or any number of characters and `?` stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either [http:///](#) or [https:///](#) or even a simple slash / as equivalent for [http:///](#)). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** [www.example.com](#) and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value [https:///](#) in the URL field, PRTG will automatically create the URL [https://www.example.com/](#)

- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL <http://www.example.com/help>
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, <http://:8080/>

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Configuration Tips for HTTP Transaction Sensors needed

- <https://kb.paessler.com/en/topic/443>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.61 HTTP XML/REST Value Sensor

The HTTP XML/REST Value sensor retrieves an XML file from a given URL and parses it.

- It can show the value of one defined XML node.

Channel	ID	Last Value	Minimum	Maximum
Downtime	-4	-4	-4	-4
Execution Time	1	280 msec	202 msec	1,873 msec
Value	0	0 #	0 #	0 #

Sensor in Other Languages

Dutch: **HTTP XML/REST Waarde**, French: **Valeur HTTP XML/REST**, German: **HTTP XML-/REST-Wert**, Japanese: **HTTP XML/REST値**, Portuguese: **Valor HTTP XML/REST**, Russian: **Значение HTTP XML/REST**, Simplified Chinese: **HTTP XML/REST ?**, Spanish: **Valor HTTP XML/REST**

Remarks

- [Requires](#) ¹⁰⁹⁰ .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- This sensor can monitor only one single node in an XML file and shows the value in one channel. If you need to monitor more than one node of an XML document, please add the sensor for each target node anew.
- Supports [Smart URL Replacement](#) ¹¹⁰⁸.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [HTTP XML/REST Value Sensor: FAQ](#)
- Knowledge Base: [Which HTTP status code leads to which HTTP sensor status?](#)
- This sensor type does not support Secure Remote Password (SRP) ciphers.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Channel Name	Enter a name for the channel that will display the value at the given URL.
--------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

URL	<p>Enter the URL that returns the XML file. It has to be URL encoded! If you enter an absolute URL, the sensor uses this address independently from the IP Address/DNS Name setting of the device on which you create this sensor.</p> <p>PRTG uses a smart URL replacement that allows you to use the parent device's IP address/DNS name setting as part of the URL.</p> <p> For more information, see section Smart URL Replacement below.</p>
-----	--

SENSOR SETTINGS

XML Node (and optional property)	<p>Enter the name of the node that this sensor checks, or enter a node name and a property name to check a property value. To obtain a value from nested tags, enter the tag names separated by a slash symbol, for example, use myTag/myTagInside as XML node value.</p> <p>i You can also check values in JavaScript Object Notation (JSON) notation. See section Checking JSON <small>1108</small> below.</p> <p>i You can try using XPath syntax here but it does not work in all cases and we do not provide any technical support for XPath issues. For further documentation about XPath, see the Knowledge Base: How can I use XPath with PRTG's XML/Rest Value Sensor?</p>
HTTP Username	If the URL requires authentication, enter the username. Please enter a string or leave the field empty.
HTTP Password	If the URL requires authentication, enter the password. Please enter a string or leave the field empty.
Sensor Value	<p>Define what value this sensor shows. Choose between:</p> <ul style="list-style-type: none"> ▪ Use the value of the selected XML node: Return the value that the sensor finds at the specified XML node. If this is non-numeric, the sensor shows 0. ▪ Use the number of occurrences of the selected XML node or its children/siblings: Return the number of occurrences found. Define further below.
Count XML Nodes	<p>This setting is only visible if you enable the return number option above. Define which count the sensor shows. Choose between:</p> <ul style="list-style-type: none"> ▪ Occurrences of the selected XML node: Return how often the defined XML node occurs at the defined URL. ▪ Child nodes of the selected XML node: Return the number of child nodes that exist below the node at the defined URL. ▪ Sibling nodes of the selected XML node: Return the number of sibling nodes that exist next to the node at the defined URL.
Namespaces	<p>Define whether namespaces in the XML document are used or not. Choose between:</p> <ul style="list-style-type: none"> ▪ Use Namespaces: Process the value you enter in the XML Node (and optional property) field including possibly existing namespace information.

SENSOR SETTINGS

- **Remove Namespaces:** Ignore namespace information in the XML document and process the value you enter in the **XML Node (and optional property)** field as node names only.

 For more information see [About Namespaces](#)¹¹⁰⁸ section below.

Content Type in Header

Define what to include in the header of the request sent to the URL defined above. Choose between:

- **Enable (recommended):** This works for most web servers and is the recommended setting.
- **Disable:** Only very few web servers cannot handle this content type and need this setting. Try this if you get an error message with the enabled option.
- **Custom:** You can use a custom content type.

Custom Content Type

This field is only visible when you enable the **Custom** option above. Enter a custom content type like `text/xml` or `text/html`.

HTTP Headers

Optionally enter a list of custom HTTP headers with their respective values that you want to transmit to the URL you define above. The syntax of a list with header-value pairs is `header1:value1|header2:value2|...|headerx:valuex`

 The sensor does not accept header field names that include a dash (-) character. If you want to use such an HTTP header, please leave out the dash of the name. For example, enter `ContentType:value` instead of `Content-Type:value`.

Example: `From:johnqpublic@example.com|AcceptLanguage:en-us`

 Ensure that the HTTP header statement is valid! Otherwise, the sensor request will not be successful.

Characters to Remove

This field is only visible if you enable the **Use the value of the selected XML node** option above. Optionally enter a string that the sensor removes from the returned XML value.

Use this to remove any unwanted characters from the result, for example, a thousands separator from numeric values. Please enter a string or leave the field empty.

Decimal Delimiter

This setting is only visible if you enable the **Use the value of the selected XML node** option above. If the sensor value of the selected XML node is of the type `float`, you can define any character here, which is then handled as the decimal delimiter. Enter one character or leave the field empty.

SENSOR SETTINGS

Custom Message	Optionally enter a custom sensor message. Use %1 as a placeholder to automatically fill in the returned XML value. Please enter a string or leave the field empty.
If Channel Value Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification ³¹⁷⁰ whenever the sensor value changes. <p> The change notification for this sensor can only be triggered if the returned value is a numerical value. Strings are not supported by this option and cannot trigger a notification.</p>
Unit String	Enter the unit for the values that this sensor returns. Please enter a string. This unit string is used for display purposes and will be shown in graphs, data tables, and gauges. If you want to change the Unit after having created the sensor, you can change it in the sensor's channel settings ³¹⁶⁰ .

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Checking JSON

With the **XML Node (and optional property)** field you can also check values that are returned in JavaScript Object Notation (JSON) notation under the defined URL.

Example

A JSON notated section may look like the following:

```
{
  "test": "Hello World",
  "object": {
    "value": "content",
    "AnotherValue": "AnotherContent"
  },
  "arraytest": [
    "one",
    "two"
  ]
}
```

Depending on your entries in the **XML Node** field, the sensor will process the respective values:

Entry in Sensor's "XML Node" Field (from Example Above)	Processed Value (from Example Above)
test	Hello World
object/value	content
object/AnotherValue	AnotherContent
object	contentAnotherContent
arraytest[1]	one
arraytest[2]	two

i The sensor converts whitespaces in JSON keys into underscores (_). So, for example, if you look for the node **some node** in the JSON, you need to enter **some_node** into the node field. If you count the number of nodes (for example, **some_node**), both **some node** and **some_node** would be counted if they appear in the JSON.

i If a key exists more than once in the JSON, the value of the first appearance is returned (no difference between whitespace and underscore).

About Namespaces

In an XML document, tags may use namespaces.

Example

A namespace notated section may look like the following:

```
<myNamespace:myNode>
  some information
</myNamespace:myNode>
```

If you set this sensor to **Use Namespaces** (this is the default setting), it will expect the full node name, including the namespace information, in the **XML Node (and optional property)** field. In the example above, this would be `myNamespace:myNode`.

If your node names are unique even without the namespace information, you can simplify the settings by setting this sensor to **Remove Namespaces**. The sensor will then expect the node name only in the **XML Node (and optional property)** field. In the example above, this would be `myNode`.

Smart URL Replacement

Instead of entering a complete address in the URL field of an HTTP sensor, you can merely enter the protocol followed by colon and three slashes (that means you can enter either `http://` or `https://` or even a simple slash `/` as equivalent for `http://`). PRTG will fill in the parent device's **IP address** or **DNS name** in front of the third slash automatically.

Whether this results in a valid URL or not depends on the IP address or DNS name of the device where this HTTP sensor is created on. In combination with cloning devices, the smart URL replacement makes it easy to create many like devices.

For example, if you create a device with **DNS name** `www.example.com` and you add an HTTP sensor to it, you can provide values the following ways:

- Providing the value `https://` in the URL field, PRTG will automatically create the URL `https://www.example.com/`
- Using the value `/help` in the URL field, PRTG will automatically create and monitor the URL `http://www.example.com/help`
- It is also possible to provide a port number in the URL field, which will be taken over by the device's DNS name and internally added, for example, `http://:8080/`

 Smart URL replacement does not work for sensors running on the **Probe Device**.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: Is there a tool available that can help me building queries for the XML/Rest Sensor?

- <https://kb.paessler.com/en/topic/48783>

Knowledge Base: How do I extract values from XML nodes (with nested tags) using PRTG's XML/Rest Value Sensor?

- <https://kb.paessler.com/en/topic/43223>

Knowledge Base: How can I use XPath with PRTG's XML/Rest Value Sensor?

- <https://kb.paessler.com/en/topic/26393>

Knowledge Base: Why does my HTTP XML/REST Value Sensor return a 404 error?

- <https://kb.paessler.com/en/topic/46503>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.62 Hyper-V Cluster Shared Volume Disk Free Sensor

The Hyper-V Cluster Shared Volume Disk Free sensor monitors a Microsoft Hyper-V cluster shared volume via PowerShell.

It can show the following:

- Available disk space in percent
- Available disk space in bytes
- Total disk space



Sensor in Other Languages

Dutch: **Hyper-V Cluster Shared Vol. Disk Free**, French: **Disque disponible Hyper-V Cluster Shared Vol.**, German: **Hyper-V Freigegebenes Clustervolumen**, Japanese: **Hyper-V クラスタ共有ボリューム ディスク空き容量**, Portuguese: **Hyper-V Disco Livre de Cluster Shared Vol.**, Russian: **Свободное дисковое пространство общего тома кластера Hyper-V**, Simplified Chinese: **Hyper-V Cluster Shared Vol. ? ? ? ? ?**, Spanish: **Espacio de disco libre de volumen compartido en clúster Hyper-V**

Remarks

- [Requires](#) Remote PowerShell on the target device.
- [Requires](#) WSFC PowerShell Interface on the target device.
- [Requires](#) .NET 4.5 or later on the probe system.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- The parent device for this sensor must be a Windows server running Hyper-V.
- Knowledge Base: [Why don't my Hyper-V sensors work after changing names?](#)
- Knowledge Base: [PowerShell Sensors: FAQ](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Remote PowerShell

 The Hyper-V Cluster Shared Volume Disk Free sensor uses PowerShell commands. To monitor devices with this sensor **Remote PowerShell** has to be enabled.

 In larger environments, the default memory limit for the remote shell might be insufficient and you might see the error message **The WSMan provider host process did not return a proper response**. In this case, increase the memory limit for Remote PowerShell. For detailed information, see the Knowledge Base article [How can I increase memory for Remote PowerShell?](#)

Requirement: WSFC PowerShell Interface

 This sensor type needs the **WSFC (Windows Server Failover Clustering) PowerShell Interface** to be installed on the target machine. You can list all modules in the PowerShell console with the command **Get-Module -ListAvailable**. Here **FailoverClusters** has to appear. Under Windows Server 2008 (not officially supported) and Windows Server 2012 the interface is part of the **VMM Administrator Console**, or the **VMM 2012 Management Console**.

The interface is available everywhere the WSFC feature is installed: Windows Server 2008 R2 (SP1) Full and Core (not installed by default); Microsoft Hyper-V Server 2008 R2 (SP1); Remote Server Administration Tools (RSAT) for Windows 10, Windows 8.1, Windows 8, Windows 7 (SP1).

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DISK FREE SETTINGS

Disk

Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 Ensure the resource name of your disks do not contain unsupported characters, especially avoid the hash (#) sign. In general, UTF-8 characters are supported. We recommend that you do not rename resource disk names once you have set up monitoring. For detailed information, see the Knowledge Base article [Why don't my Hyper-V sensors work after changing names?](#)

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)¹⁸¹, as well as in [alarms](#)²¹⁹, [logs](#)²²⁸, [notifications](#)³²¹⁶, [reports](#)³²⁵², [maps](#)³²⁷⁸, [libraries](#)³²³⁵, and [tickets](#)²³⁰.

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DISK FREE SETTINGS

Disk	Shows the name of the disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage.  This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- <https://kb.paessler.com/en/topic/15533>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
62 Hyper-V Cluster Shared Volume Disk Free Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

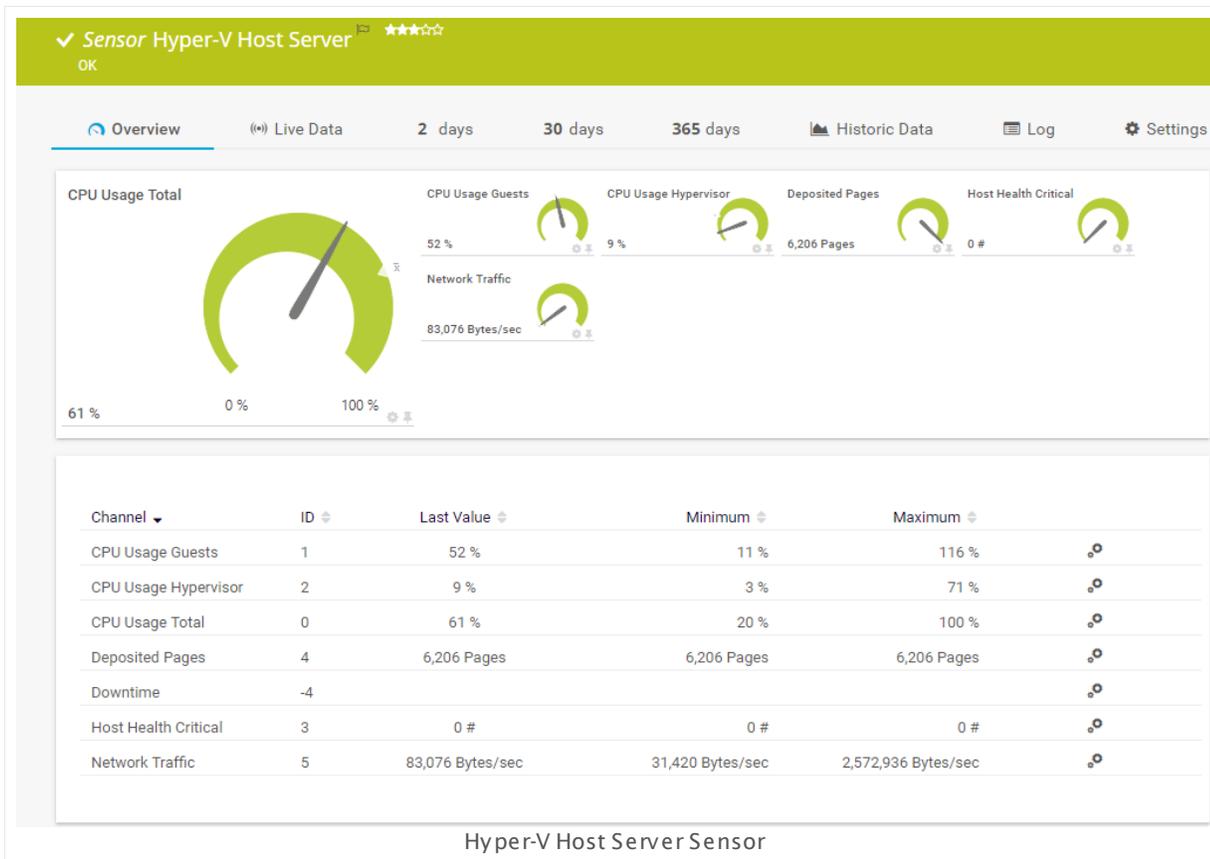
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.63 Hyper-V Host Server Sensor

The Hyper-V Host Server sensor monitors a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- CPU usage in percent of guests, hypervisor, total
- Number of host health critical values
- Number of deposited pages
- Network traffic: Sums up the total bytes per second (received and sent) on all ports of your virtual switch.



Sensor in Other Languages

Dutch: **Hyper-V Host Server**, French: **Serveur hôte Hyper V**, German: **Hyper-V Host Server**, Japanese: **Hyper-Vホストサーバー**, Portuguese: **Hyper-V Host**, Russian: **Сервер узла Hyper-V**, Simplified Chinese: **Hyper-V ? ? ? ? ?**, Spanish: **Servidor Hyper-V Host**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - [Requires](#) ¹¹²² Windows Server 2008 R2 or later on the probe system.
 - [Requires](#) ¹¹²³ the Remote Registry Windows service to be running on the target computer.
 - The parent device for this sensor must be a Windows server running Hyper-V.
 - Can use a [hybrid approach](#) ¹¹²⁴ with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ⁴⁰⁷ **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#) ⁴¹⁵ on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#) ¹²⁵. Above this number, please consider using multiple [Remote Probes](#) ³⁷⁰⁹ for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#) ³⁵⁰⁷ section.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#) ³⁷⁰⁵.

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

x In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result**: Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

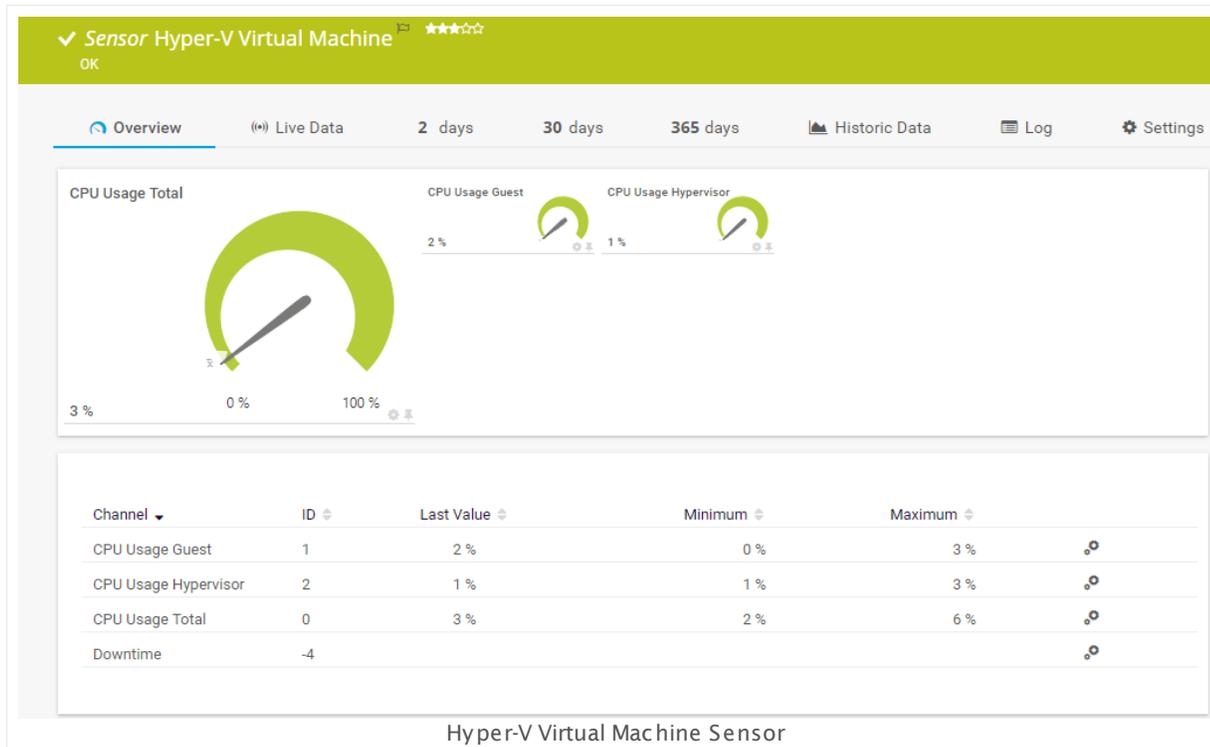
7.8.64 Hyper-V Virtual Machine Sensor

The Hyper-V Virtual Machine sensor monitors a virtual machine running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- CPU usage in percent of guests, hypervisor, total
- IDE disk read speed (bytes per second)
- IDE disk write speed (bytes per second)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Virtuele Hyper-V-Machine**, French: **Machine virtuelle Hyper V**, German: **Hyper-V Virtuelle Maschine**, Japanese: **Hyper-V 仮想マシン**, Portuguese: **Hyper-V Máquina Virtual**, Russian: **Виртуальная машина Hyper-V**, Simplified Chinese: **Hyper-V 虚拟机**, Spanish: **Máquina virtual Hyper-V**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- [Requires](#) ¹¹³² Windows Server 2008 R2 or later on the probe system.
 - [Requires](#) ¹¹³² the Remote Registry Windows service to be running on the target computer.
 - The parent device for this sensor must be a Hyper-V server.
 - The sensor does not support **Live Migration**.
 - Can use a [hybrid approach](#) ¹¹³¹ with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
 - To monitor a virtual machine with this sensor, disable User Account Control (UAC) in the control panel of the Windows operating system that is running on this virtual machine. Otherwise, the sensor might switch into a **Down** status with the error message **The virtual machine is not running or is powered off**.
 - Knowledge Base: [Why don't my Hyper-V sensors work after changing names?](#)
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ⁴⁰⁷ **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#) ⁴¹⁵ on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#) ¹²⁵. Above this number, please consider using multiple [Remote Probes](#) ³⁷⁰⁹ for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#) ³⁵⁰⁷ section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)³⁷⁰⁸.

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the virtual machines you want to monitor. PRTG creates one sensor for each VM you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine	Select the virtual machines (VMs) you want to add a sensor for, including the ones that are not running. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-----------------	---

VIRTUAL MACHINE SETTINGS

 Ensure the name of your VMs do not contain unsupported characters, especially avoid the hash (#) sign. We recommend to not rename virtual machines once you have set up monitoring. For detailed information, see the Knowledge Base article [Why don't my Hyper-V sensors work after changing names?](#)

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VIRTUAL MACHINE SETTINGS

GUID	Shows the Globally Unique Identifier (GUID) of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	Shows information about the virtual machine. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Powered Off VMs	Define how to react to a virtual machine that is powered off. Choose between: <ul style="list-style-type: none">• Alarm when powered off: The sensor will change to a Down status ^[195] if the virtual machine is powered off. While in Down status, a sensor does not record any data in any of its channels.• Ignore powered off state: The sensor will not change to a Down status ^[195] if the virtual machine is powered off. It will report zero values instead.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.<ul style="list-style-type: none">📁 For more information on how to find the folder used for storage, see section Data Storage ^[3734].☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Why don't my Hyper-V sensors work after changing names?

- <https://kb.paessler.com/en/topic/15533>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
64 Hyper-V Virtual Machine Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

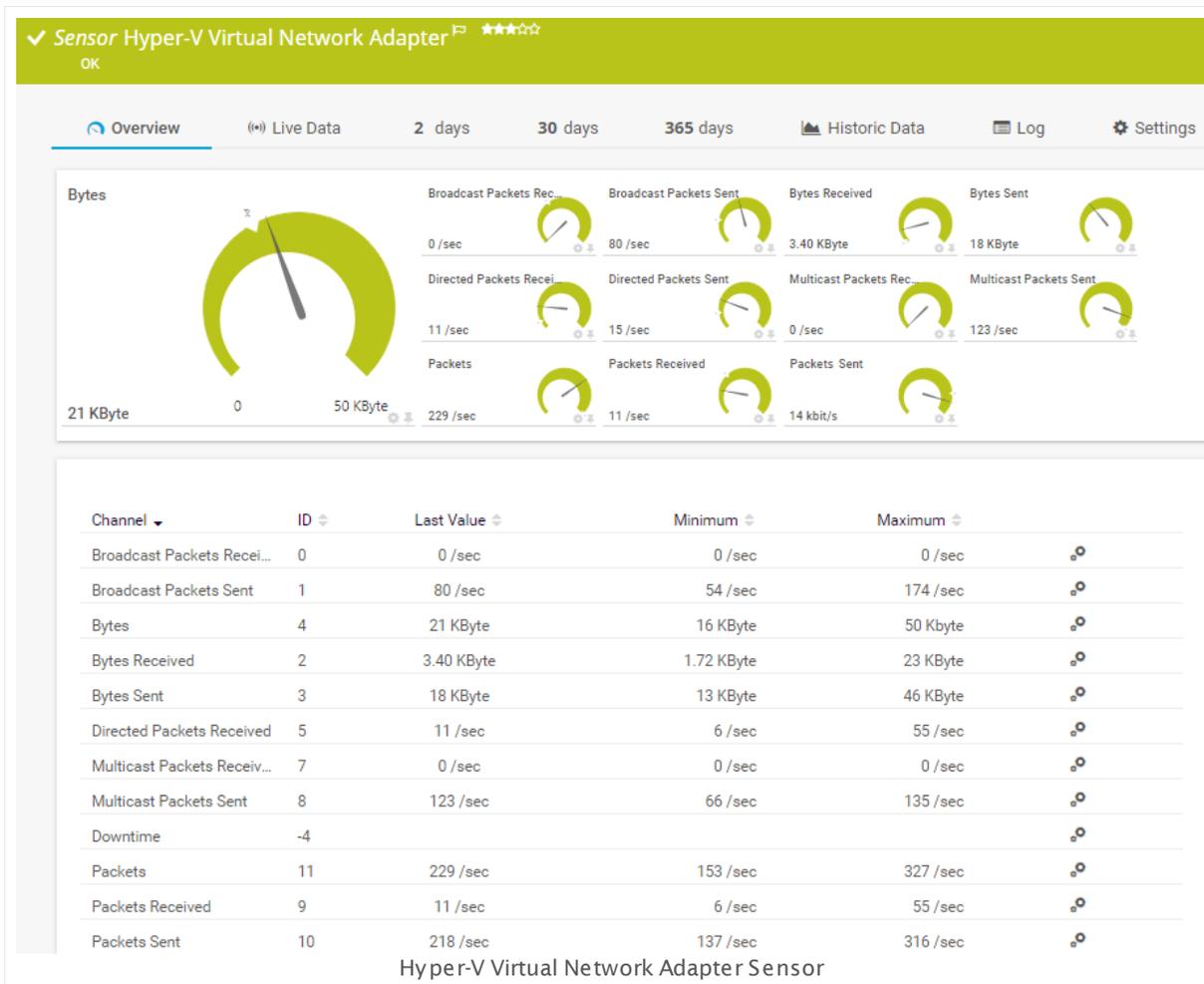
7.8.65 Hyper-V Virtual Network Adapter Sensor

The Hyper-V Network Adapter sensor monitors virtual network adapters running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Sent, received, and totally transferred bytes
- Sent and received packets per second
- Sent and received broadcast packets per second
- Sent and received directed packets per second
- Sent and received multicast packets per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Hyper-V Virtuele Netwerk Adapter**, French: **Carte réseau virtuel Hyper-V**, German: **Hyper-V Virtueller Netzwerkadapter**, Japanese: **Hyper-V 仮想ネットワークアダプター**, Portuguese: **Hyper-V Adaptador de Rede Virtual**, Russian: **Виртуальный сетевой адаптер Hyper-V**, Simplified Chinese: **Hyper-V ? ? ? ? ? ? ?**, Spanish: **Adaptador de red virtual Hyper-V**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- [Requires](#)^[1143] Windows Server 2008 R2 or later on the probe system.
- [Requires](#)^[1143] the Remote Registry Windows service to be running on the target computer.
- The parent device for this sensor must be a Hyper-V server.
- Can use a [hybrid approach](#)^[1142] with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
- Knowledge Base: [Why don't my Hyper-V sensors work after changing names?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)³⁷⁰⁸.

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵¹ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network adapters you want to monitor. PRTG creates one sensor for each adapter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Hyper-V Virtual
Network Adapter

Select the virtual network adapters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

VIRTUAL MACHINE SETTINGS

 We recommend you do not rename virtual machines once you have set up monitoring. Renaming them will also change the internal virtual network adapter names, so monitoring might be interrupted. For detailed information about virtual machine naming, see the Knowledge Base article [Why don't my Hyper-V sensors work after changing names?](#)

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HYPER-V VIRTUAL NETWORK ADAPTER SETTINGS

Virtual Network Adapter Shows the name of the virtual network adapter monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Why don't my Hyper-V Virtual Machine sensors work after changing names?

- <https://kb.paessler.com/en/topic/15533>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

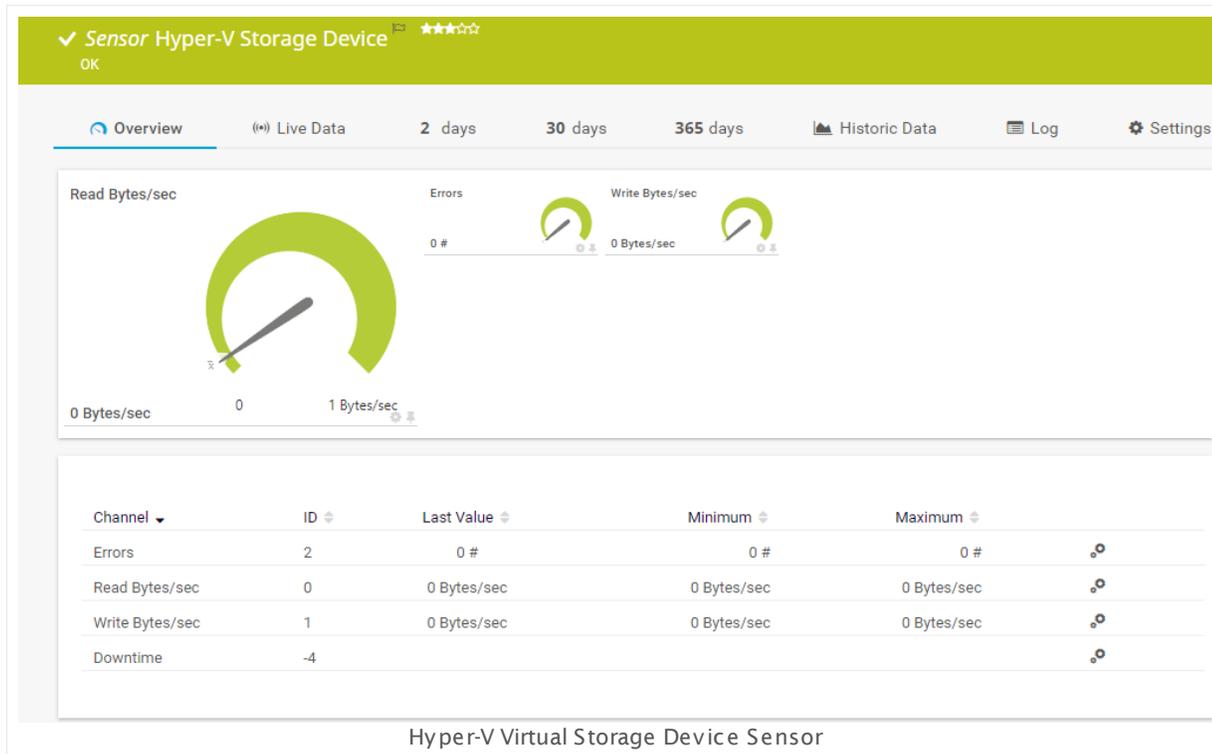
7.8.66 Hyper-V Virtual Storage Device Sensor

The Hyper-V Virtual Storage sensor monitors a virtual storage device running on a Microsoft Hyper-V host server via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Read speed in bytes per second
- Write speed in bytes per second
- Number of errors

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Hyper-V Virtueel Opslag Apparaat**, French: **Périphérique de stockage virtuel Hyper-V**, German: **Hyper-V Virtuelles Speichergerät**, Japanese: **Hyper-V仮想ストレージデバイス**, Portuguese: **Hyper-V Dispositivo de Armazenamento Virtual**, Russian: **Виртуальное устройство хранения Hyper-V**, Simplified Chinese: **Hyper-V ? ? ? ? ?**, Spanish: **Dispositivo de almacenamiento virtual Hyper-V**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - [Requires](#) ^[1154] Windows Server 2008 R2 or later on the probe system.
 - [Requires](#) ^[1154] the Remote Registry Windows service to be running on the target computer.
 - The parent device for this sensor must be a Hyper-V server.
 - This sensor does not support **Live Migration**.
 - Can use a [hybrid approach](#) ^[1153] with Windows Performance Counters and WMI as fallback to query data. Please stay below 200 WMI sensors per probe!
 - Knowledge Base: [Why don't my Hyper-V sensors work after changing names?](#)
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#) ^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#) ^[125]. Above this number, please consider using multiple [Remote Probes](#) ^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#) ^[3507] section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)³⁷⁰⁸.

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the storage devices you want to monitor. PRTG creates one sensor for each storage you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HYPER-V VIRTUAL STORAGE DEVICE SETTINGS

Virtual Storage Device	Select the virtual storage devices you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HYPER-V VIRTUAL STORAGE DEVICE SETTINGS

Virtual Storage Device	Shows the unique identifier of the device that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> 📁 For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> 📘 This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

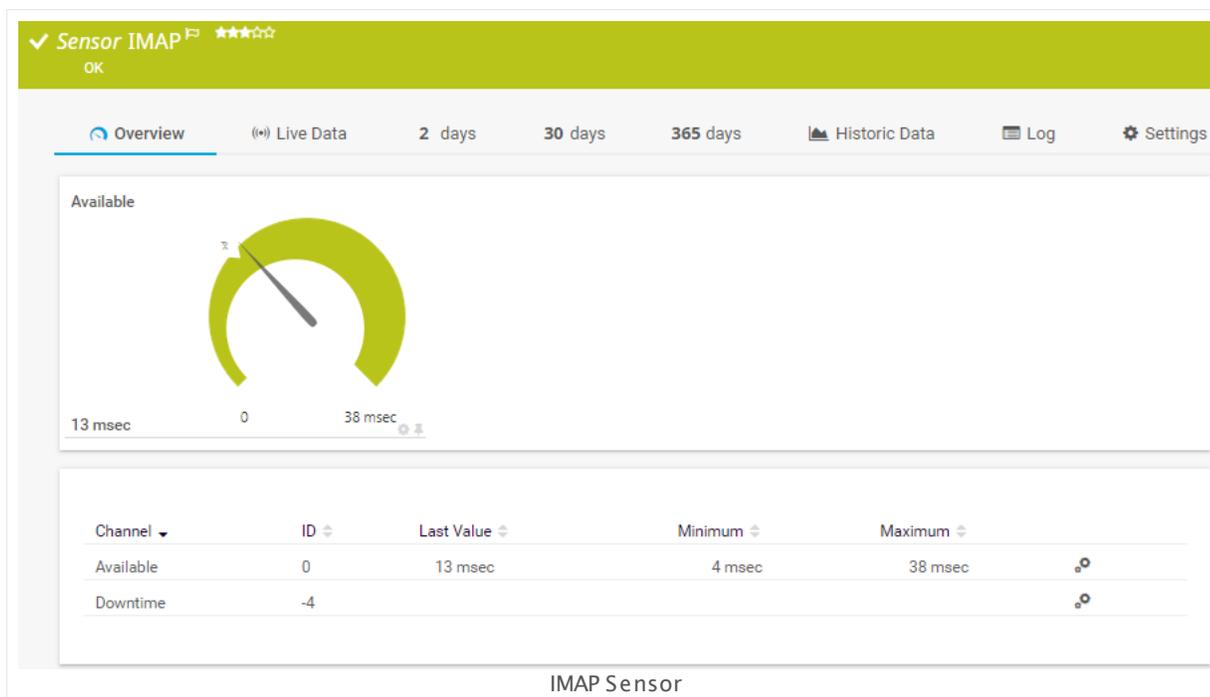
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.67 IMAP Sensor

The IMAP sensor monitors an email server using Internet Message Access Protocol (IMAP).

It can show the following:

- Response time of the email server
- Number of emails in the defined mailbox
- It can also check the content of emails for certain key words. This way, you can use this sensor to monitor backup solutions via emails that are sent out by these solutions. For more information, see the Knowledge Base article [How can I monitor my backup software to be sure backup succeeded last night?](#)



Remarks

- If you use content checks, we recommend using a dedicated IMAP account that is only checked by PRTG. Editing existing mails in the mailbox of the monitored IMAP account can lead to false alarms or malfunctions of this sensor type.
- This sensor type might not work properly when monitoring subfolders of mailboxes. If it has to check subsequent emails with identical subjects, later on incoming emails might not be recognized.
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- Knowledge Base: [My IMAP sensor does not process HTML emails correctly using regex. What can I do?](#)
- Knowledge Base: [How can I monitor my backup software to be sure backup succeeded last night?](#)

- Knowledge Base: [Can I analyze multipart emails using the PRTG IMAP sensor?](#)
- Knowledge Base: [My IMAP sensor does not find emails when I check for message date. What can I do?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CONNECTIVITY

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

Port Enter the number of the port that the sensor uses to connect via IMAP. For non-secure connections, usually port 143 is used. For SSL connections it is usually port 993. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value.

 If you do not get a connection, please try another port number.

Security Define the security level for the sensor connection. Choose between:

- **Use Transport-Level Security if available using StartTLS (default):** Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
- **Use Transport-Level Security if available:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
- **Enforce Transport-Level Security using StartTLS:** Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down status**^[195].
- **Enforce Transport-Level Security:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down status**^[195].

 If the sensor connects to a server via **StartTLS**, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.

CONNECTIVITY

-  If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

AUTHENTICATION

- Username** Enter a username for IMAP authentication. Please enter a string.
- Password** Enter a password for IMAP authentication. Please enter a string.
- Mailbox Name** Enter the name of the mailbox (for example, the name of the IMAP folder) that the sensor will check. Default value is **Inbox**. Unless you set a last message date check below, the sensor will always look at **all** emails contained in the mailbox.
-  Ensure you do not manually edit emails in this mailbox with another email client because this can result in malfunctions of this sensor's email identification.

SENSOR BEHAVIOR

- General Behavior** This sensor can additionally check the content of all incoming emails. Choose between:
- **Check connectivity only, do not process emails (default):** Only check availability of the IMAP server and check if a login is successful. Do not process any emails in the IMAP email account.
 - **Count emails in this mailbox:** Count the emails in the defined mailbox.
 - **Process emails in this mailbox:** Log in to the IMAP email account and check the emails that it contains. Define further options below.
- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.

SENSOR BEHAVIOR

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

FILTER EMAILS IN INBOX

📘 This settings section is only visible if you choose to process the emails in the mailbox.

Only Include Emails with Matching "From"

Define if you want to check the "From" field of the emails. When using a search, the sensor will scan all emails from the newest to the oldest. Choose between:

- **Do not check (default):** Do not process this field in emails.
- **Check using string search:** Process this field in emails using simple string search.
- **Check using regular expression:** Process this field in emails using a regular expression.

⚠ PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)³⁷⁰⁴.

📘 The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.

Search for

This field is only visible if you enable a "from" check above. Enter a search string using the method defined above.

Only Include Emails with Matching "Subject"

Define if you want to check the "Subject" field of the emails. When using a search, the sensor will scan all emails from the newest to the oldest. Choose between:

- **Do not check (default):** Do not process the subject of emails.

FILTER EMAILS IN INBOX

- **Check using string search:** Process the subject of emails using simple string search.
- **Check using regular expression:** Process the subject of emails using a regular expression. For more information about syntax, see the [Regular Expressions](#) ³⁷⁰⁴ section.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) ³⁷⁰⁴.

 The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.

Search for

This field is only visible if you enable a "subject" check above. Enter a search string using the method defined above.

Only Include Emails with Matching Email Body

Define if you want to check the email body of the emails. When using a search, the sensor will scan all emails from the newest to the oldest. Choose between:

- **Do not check (default):** Do not process the email body.
- **Check using string search:** Process the email body using simple string search.
- **Check using regular expression:** Process the email body using a regular expression. For more information about syntax, see the [Regular Expressions](#) ³⁷⁰⁴ section.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#) ³⁷⁰⁴.

 The sensor finishes the scan with the first match! This means that after it has found a match in one email, the sensor will not perform any further checks in older emails.

Search for

This field is only visible if you enable checking the email body above. Enter a search string using the method defined above.

Only Include Recent Emails

Define if you want to check all emails in the mailbox, or only mails that were received within the last few hours. Choose between:

- **Do not check message age (default):** Always check all emails that the mailbox contains.
- **Emails must be younger than:** Only check emails that were received in the last few hours. Define below.

FILTER EMAILS IN INBOX

Maximum Age in Hours	This field is only visible if you enable the message age check above. Enter the maximum age in hours. The sensor will only process emails that are younger. Please enter an integer value.
If No Email Matches the Above Filters	Define which status ¹⁹⁵ the sensor will show if it does not find any email in the mailbox that matches the defined filters. Choose between: <ul style="list-style-type: none"> ▪ Set sensor to "Up" status (default) ▪ Set sensor to "Warning" status ▪ Set sensor to "Down" status
Message	This field is only visible if you define a Warning or Down status as no matching behavior above. Define the message that the sensor will show if it did not find any matching emails together with a Warning or Down status as you define above.

VALIDATE LATEST EMAIL

-  This settings section is only visible if you choose to process the emails in the mailbox.
-  The sensor will only validate the latest email that matches the filters above! If the sensor does not find a matching email, it will not perform any email validation.

For the Latest Email that Matches, Set Sensor to "Warning" Status	Define in which cases the sensor will show a Warning status ¹⁹⁵ . Choose between: <ul style="list-style-type: none"> ▪ Never (default): Never set this sensor to a Warning status based on email content. ▪ Always: Always set this sensor to a Warning status in case any emails could be identified. ▪ If subject contains: Set the sensor to Warning if the subject of the found email contains the search text you define below. ▪ If subject does not contain: Set the sensor to Warning if the subject of the found email does not contain the search text you define below. ▪ If email body contains: Set the sensor to Warning if the body of the found email contains the search text you define below.
---	---

VALIDATE LATEST EMAIL

	<ul style="list-style-type: none"> ▪ If email body does not contain: Set the sensor to Warning if the body of the found email does not contain the search text you define below.
Check Method	<p>This setting is only visible if you select an if condition above. Define how you want to check for the above condition. Choose between:</p> <ul style="list-style-type: none"> ▪ String search: Check the email subject or body using simple string search. ▪ Regular expression: Check the email subject or body using a regular expression. For more information about syntax, see Regular Expressions^[3704] section. <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions^[3704].</p>
Search Text	<p>This setting is only visible if you select an if condition above. Enter a search string using the method defined above.</p>
Warning Message	<p>This setting is only visible if you select a warning condition above. Define the message that the sensor will show for a Warning status^[195].</p>
Based on Message Age, Set Sensor to "Warning" Status	<p>Define if you want to check the age of the latest matching email in the mailbox. Choose between:</p> <ul style="list-style-type: none"> ▪ Never (default): Do not check the age of the email. ▪ If email is older than: Set the sensor to Warning status^[195] if the found email is older than you define below.
Message Age in Hours	<p>This field is only visible if you enable the message age check above. Enter the maximum age in hours. If the processed email is older, the sensor will show a Warning status^[195]. Please enter an integer value.</p> <p> Ensure you do not manually edit emails in this mailbox with another email client because this can result in malfunctions of the message age check.</p>
For the Latest Email that Matches, Set Sensor to "Down" Status	<p>Define in which cases the sensor will show a Down status^[195]. Choose between:</p> <ul style="list-style-type: none"> ▪ Never (default): Never set this sensor to a Down status based on email content.

VALIDATE LATEST EMAIL

- **Always:** Always set this sensor to a **Down** status in case any emails could be identified.
- **If subject contains:** Set the sensor to **Down** if the subject of the found email contains the search text you define below.
- **If subject does not contain:** Set the sensor to **Down** if the subject of the found email does not contain the search text you define below.
- **If email body contains:** Set the sensor to **Down** if the body of the found email contains the search text you define below.
- **If email body does not contain:** Set the sensor to **Down** if the body of the found email does not contain the search text you define below.

Check Method

This setting is only visible if you select an if condition above. Define how you want to check for the above condition. Choose between:

- **String search:** Check the email subject or body using simple string search.
- **Regular expression:** Check the email subject or body using a regular expression. For more information about syntax, see [Regular Expressions](#)^[3704] section.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

Search Text

This setting is only visible if you enable an if condition above. Enter a search string using the method defined above.

Error Message

This setting is only visible if you select a down condition above. Define the message that the sensor will show for a **Down status**^[195].

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I monitor my backup software to be sure backup succeeded last night?

- <https://kb.paessler.com/en/topic/47023>

Knowledge Base: My IMAP sensor does not process HTML emails correctly using regex. What can I do?

- <https://kb.paessler.com/en/topic/61019>

Knowledge Base: Can I analyze multipart emails using the PRTG IMAP sensor?

- <https://kb.paessler.com/en/topic/63532>

Knowledge Base: My IMAP sensor does not find emails when I check for message date. What can I do?

- <https://kb.paessler.com/en/topic/69811>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

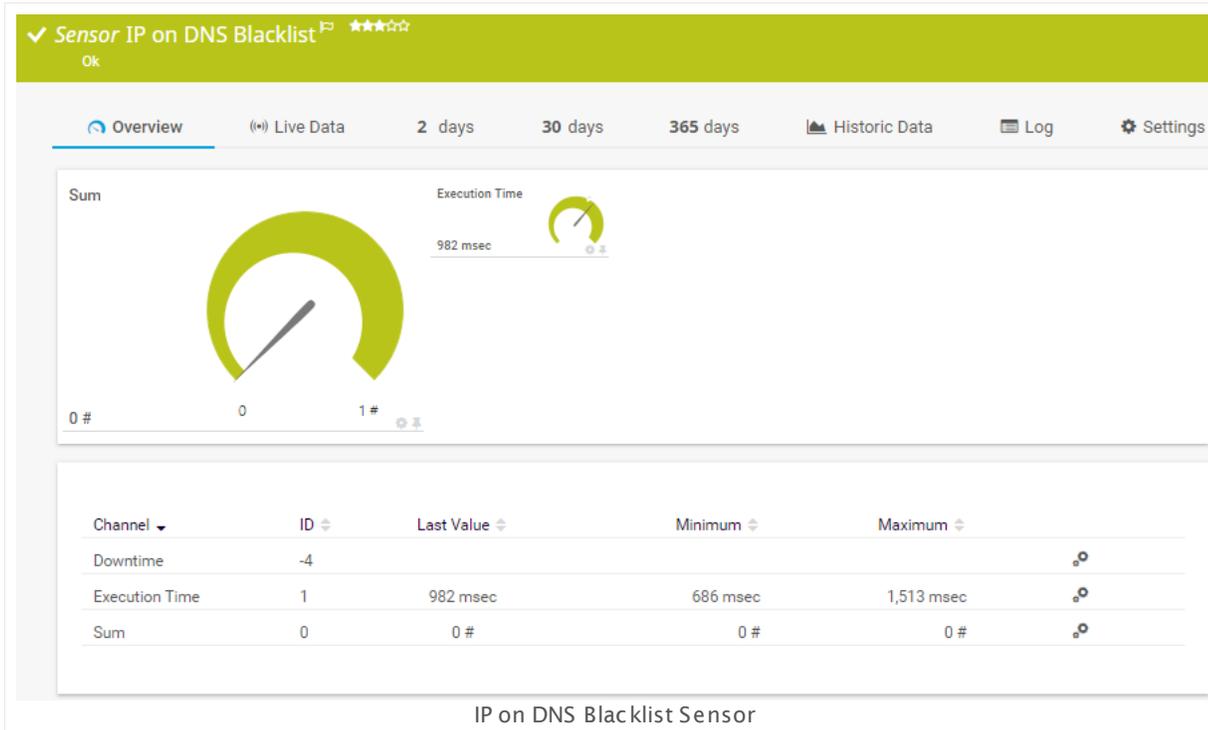
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.68 IP on DNS Blacklist Sensor

The IP on DNS Blacklist sensor checks if the IP address of its parent device is listed on specific blacklist servers.

- The sensor shows the number of blacklist hits it can find.



Sensor in Other Languages

Dutch: **IP op DNS Blacklist**, French: **IP sur liste noire du DNS**, German: **IP auf Schwarzer Liste des DNS**, Japanese: **DNS ブラックリスト記載のIP**, Portuguese: **IP em Blacklist DNS**, Russian: **Черный список IP-адресов на DNS**, Simplified Chinese: **DNS ??? IP**, Spanish: **Blacklist IP sobre DNS**

Remarks

- If a DNS name is used as hostname of the parent device, PRTG will resolve it to an IP address before querying blacklist servers.
- During normal operation, there should be 0 hits and the sensor should show a green **Up status**. If the sensor can find the IP address on at least one of the blacklist servers, it will show a yellow **Warning** status by default. You can set additional thresholds in the **Sensor Channels Settings**.
- **Requires** .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [Is there a list of anti spam black list servers?](#)

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more **Tags**^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically **inherited**^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

- Blacklist Servers** Define the blacklist servers that the sensor uses for the check. You can enter a comma separated list. Default is **bl.spamcop.net**.
-  For a list of servers, see this Knowledge Base article: [Is there a list of anti spam black list servers?](#)
-  With each scanning interval, PRTG will query all servers in the list! We recommend you do not enter more than 10 servers to make sure the check can be completed within the scanning interval of this sensor. If you use too many blacklist servers, the sensor will show the error message **Timeout (code: PE018)**.

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

- i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Is there a list of anti spam black list servers?

- <https://kb.paessler.com/en/topic/37633>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

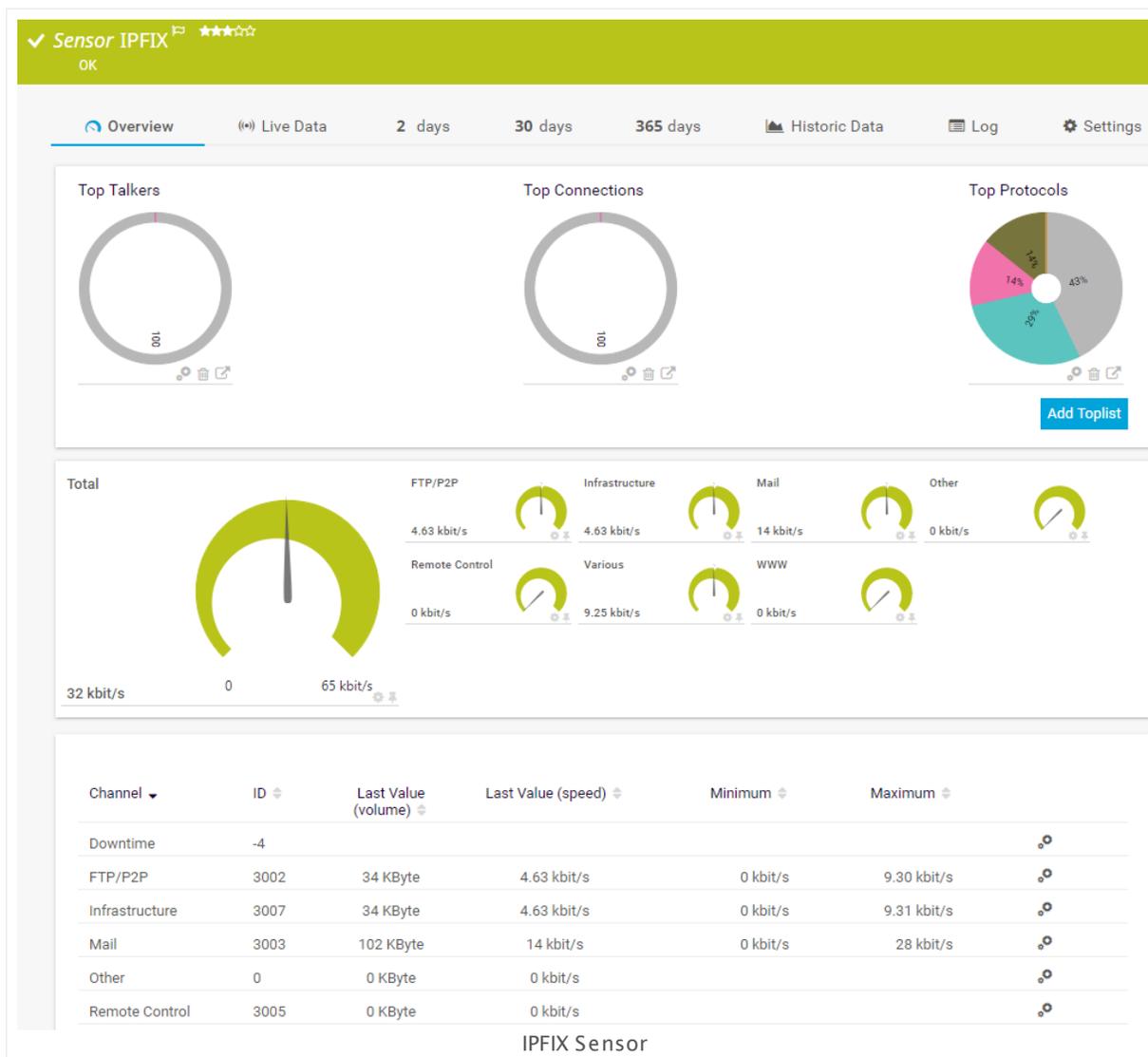
7.8.69 IPFIX Sensor

The IPFIX sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows traffic by type. There are several filter options available to divide traffic into different channels. Ensure your device supports IPFIX when using this sensor.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- You have to enable IPFIX export on the device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)
- Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
- For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#).

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPFIX SPECIFIC SETTINGS

Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	<p>Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup.</p> <p>To select an IP address, add a check mark in front of the respective line or in the top level box to select all. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an Unknown status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device.</p> <p> For more details about this setting, see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?</p> <p> If you set this value too low, flow information might be lost!</p>
Sampling Mode	<p>Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:</p> <ul style="list-style-type: none"> ▪ Off: The standard flow will be used. ▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	This field is only visible when sampling mode is On above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.
Log Stream Data to Disk (for Debugging)	Define if you want the probe to write a logfile of the stream and packet data to the data folder (see Data Storage ³⁷³⁴). Choose between:

IPFIX SPECIFIC SETTINGS

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
 - **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
 - **All stream data:** Write logfiles for all data received.
-  Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.

CHANNEL CONFIGURATION

- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.

 Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#) ¹¹⁹⁷ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#) ¹¹⁹⁷ below.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[3160] settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplist you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
69 IPFIX Sensor

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to IPFIX sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).

FIELD	POSSIBLE FILTER VALUES
NextHop	IP address or DNS name (see Valid Data Formats )
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

More

Paessler Website: Paessler NetFlow Testers

- <https://www.paessler.com/tools/netflowtester>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)  section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)  section.

Others

For more general information about settings, see the [Object Settings](#)  section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#) 

7.8.70 IPFIX (Custom) Sensor

The IPFIX (Custom) sensor receives traffic data from an IPFIX (Internet Protocol Flow Information Export) compatible device and shows the traffic by type. In this custom sensor, you can define your own channel definitions to divide traffic into different channels. Ensure your device supports IPFIX when using this sensor.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor IPFIX ★★★★☆
OK

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Top Talkers

Top Connections

Top Protocols

[Add Toplist](#)

Total

FTP/P2P	4.63 kbit/s	Infrastructure	4.63 kbit/s	Mail	14 kbit/s	Other	0 kbit/s
Remote Control	0 kbit/s	Various	9.25 kbit/s	WWW	0 kbit/s		

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
FTP/P2P	3002	34 KByte	4.63 kbit/s	0 kbit/s	9.30 kbit/s
Infrastructure	3007	34 KByte	4.63 kbit/s	0 kbit/s	9.31 kbit/s
Mail	3003	102 KByte	14 kbit/s	0 kbit/s	28 kbit/s
Other	0	0 KByte	0 kbit/s		
Remote Control	3005	0 KByte	0 kbit/s		

IPFIX Sensor

Sensor in Other Languages

Dutch: **IPFIX (aangepast)**, French: **IPFIX (Personnalisé)**, German: **IPFIX (Benutzerdef.)**,
Japanese: **IPFIX (カスタム)**, Portuguese: **IPFIX (customizado)**, Russian: **IPFIX (нестандартный)**,

Simplified Chinese: IPFIX (? ? ?), Spanish: **IPFIX (personalizado)**

Remarks

- In order for this sensor to work, you have to enable IPFIX export on the device. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
 - This sensor [does not support more than 50 channels](#)¹²⁰¹ officially.
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPFIX SPECIFIC SETTINGS

Receive IPFIX Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one configured in the IPFIX export options of your hardware router device. Please enter an integer value.
Sender IP	Enter the IP address of the sending device you want to receive the IPFIX data from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.
Receive IPFIX Packets on IP	Select the IP address(es) on which PRTG listens to IPFIX packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the IPFIX export options of your hardware router device.

IPFIX SPECIFIC SETTINGS

Active Flow Timeout (Minutes) Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data is received, the sensor may switch to an **Unknown status** ^[195]. Please enter an integer value.

We recommend you set this one minute longer than the respective timeout configured in your hardware router device.

 For more details about this setting, see this Knowledge Base article: [What is the Active Flow Timeout in Flow sensors?](#)

 If you set this value too low, flow information might be lost!

Sampling Mode Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:

- **Off:** The standard flow will be used.
- **On:** Switch into sampling mode and specify the sampling rate below.

Sampling Rate This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Channel Definition Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined will be accounted to the default channel named **Other**.

 For detailed information, see section [Channel Definitions for xFlow and Packet Sniffer Sensors](#) ^[369].

 Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.

Log Stream Data to Disk (for Debugging) Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#) ^[374]). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.

IPFIX SPECIFIC SETTINGS

- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

FILTERING

Include Filter	<p>Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.</p>
----------------	--

FILTERING

 For detailed information, see section [Filter Rules](#)¹²¹⁰ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹²¹⁰ below.

PRIMARY TOPLIST

Primary Toplist

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplists you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to IPFIX sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).

FIELD	POSSIBLE FILTER VALUES
NextHop	IP address or DNS name (see Valid Data Formats )
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

More

Paessler Website: Paessler NetFlow Testers

- <https://www.paessler.com/tools/netflowtester>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)  section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)  section.

Others

For more general information about settings, see the [Object Settings](#)  section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#) 

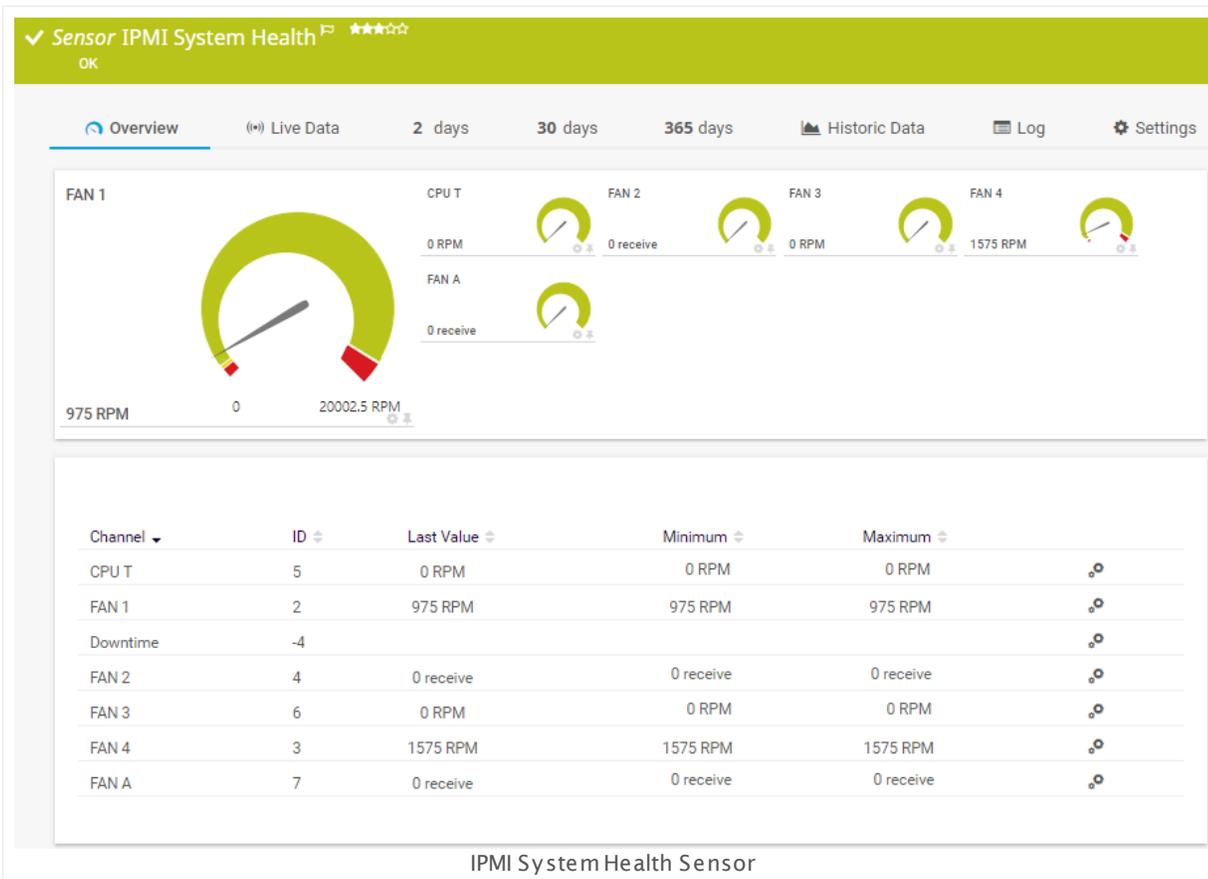
7.8.71 IPMI System Health Sensor

The IPMI System Health sensor monitors the status of a system via the Intelligent Platform Management Interface (IPMI).

It can show the following:

- Temperatures of, for example, the system or the peripheral temperature.
- Fan rotation per minute
- Voltages
- Status of a power supply

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **IPMI System Health**, French: **État du système IPMI**, German: **IPMI Systemzustand**, Japanese: **IPMI システムヘルス**, Portuguese: **Funcionamento do sistema via IPMI**, Russian: **Работоспособность системы IPMI**, Simplified Chinese: **IPMI ? ? ? ?**, Spanish: **Estado del sistema IPMI**

Remarks

- You have to explicitly specify the credentials of the IPMI in the sensor settings.
 - [Requires](#) ¹²¹⁴ .NET 4.5 or later on the probe system.
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#) ³⁶⁹³.
 - This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#) ³¹⁶⁰.
 - Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Before you can actually add this sensor, PRTG will ask you to provide your credentials for the Intelligent Platform Management Interface (IPMI) in the **Add Sensor** dialog. Enter the **Username** and the **Password** in the respective fields.

Select the metrics you want to monitor. PRTG will create one sensor for each metric you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IPMI SPECIFIC

Group Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IPMI CREDENTIALS

Username Enter the username for the Intelligent Platform Management Interface (IPMI). If not changed yet, this field shows the username that you defined during sensor creation.

Password Enter the password for the Intelligent Platform Management Interface (IPMI). If not changed yet, this field shows the encrypted password that you defined during sensor creation.

IPMI SPECIFIC

Group Shows the metric that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Logfile Results Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.72 jFlow V5 Sensor

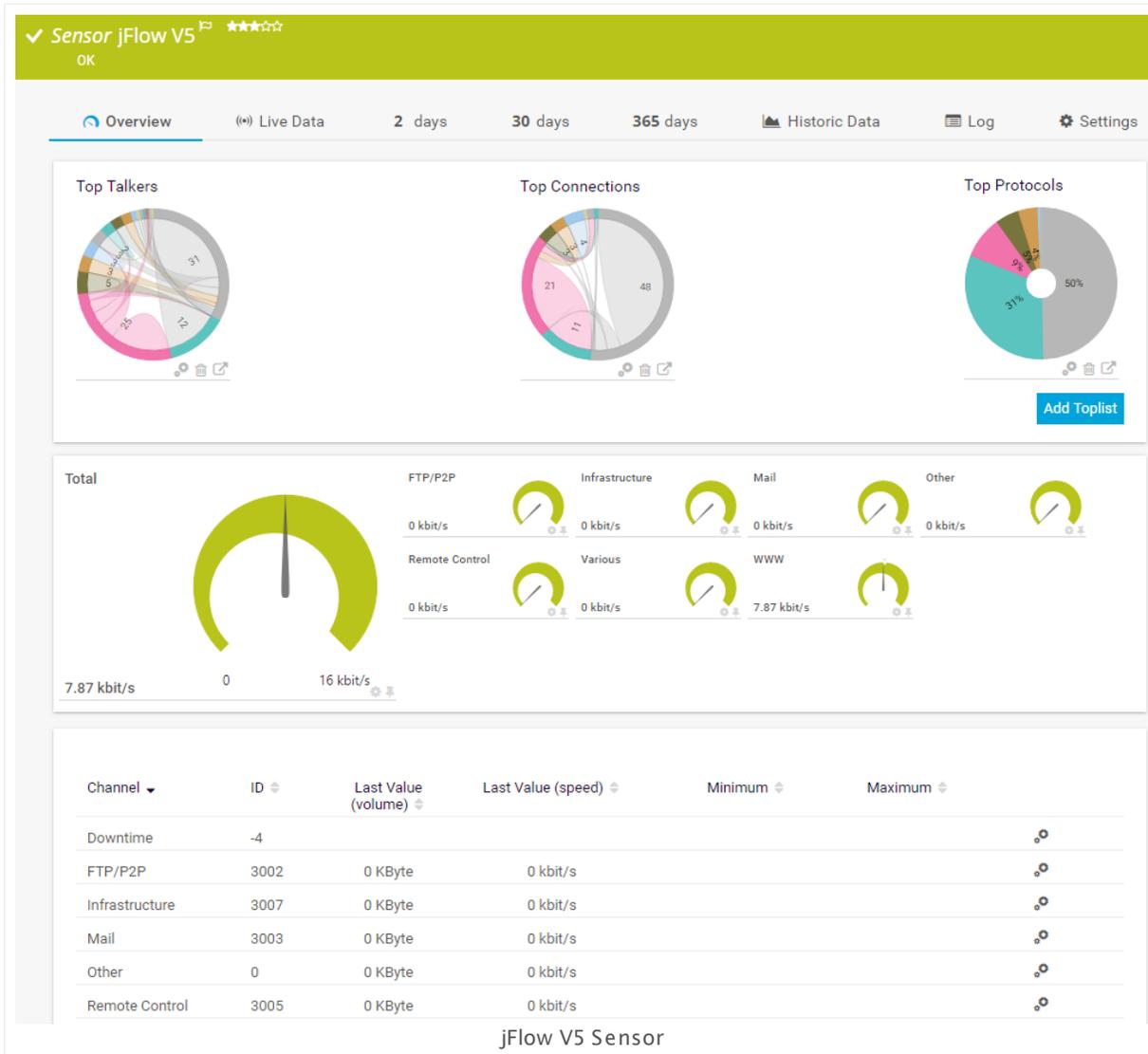
The jFlow V5 sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, ensure it matches jFlow V5! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
72 jFlow V5 Sensor



Remarks

- You have to enable jFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#).
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

JFLOW V5 SPECIFIC SETTINGS

Receive jFlow Packets on UDP Port	<p>Enter the UDP port number on which PRTG receives the flow packets. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value.</p> <p> When you configure the export, make sure you select the appropriate jFlow version for this sensor.</p>
Sender IP	<p>Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.</p>
Receive jFlow Packets on IP	<p>Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head.</p> <p>The IP address you select here must match the one you configured in the jFlow export options of your hardware router device.</p> <p> When you configure the export, make sure you select the appropriate jFlow version for this sensor.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must have received new flow data. If the timeout is reached and no new data came in, the sensor may switch to an Unknown status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device.</p> <p> For more details about this setting, see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?</p> <p> If you set this value too low, flow information might be lost!</p>
Sampling Mode	<p>Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:</p> <ul style="list-style-type: none">▪ Off: The standard flow will be used.▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	<p>This field is only visible when sampling mode is On above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.</p>

JFLOW V5 SPECIFIC SETTINGS

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.

CHANNEL CONFIGURATION

- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.
- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
 - ⚠ Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.
 - 💡 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

FILTERING

- Include Filter** Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.
- 🔍 For detailed information, see section [Filter Rules](#)¹²³⁴ below.
- Exclude Filter** First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.
- 🔍 For detailed information, see section [Filter Rules](#)¹²³⁴ below.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[3160] settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplists you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) ³³⁶⁵ on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status** ¹⁹⁵¹. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) ³⁶⁸³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to jFlow V5 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number

More

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.73 jFlow V5 (Custom) Sensor

The jFlow V5 (Custom) sensor receives traffic data from a jFlow V5 compatible device and shows the traffic by type. On your hardware device, please make sure it matches jFlow V5! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor jFlow V5 ★★★★☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Top Talkers

Top Connections

Top Protocols

[Add Toplist](#)

Total

7.87 kbit/s

FTP/P2P

0 kbit/s

Infrastructure

0 kbit/s

Mail

0 kbit/s

Other

0 kbit/s

Remote Control

0 kbit/s

Various

0 kbit/s

WWW

7.87 kbit/s

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
FTP/P2P	3002	0 KByte	0 kbit/s		
Infrastructure	3007	0 KByte	0 kbit/s		
Mail	3003	0 KByte	0 kbit/s		
Other	0	0 KByte	0 kbit/s		
Remote Control	3005	0 KByte	0 kbit/s		

jFlow V5 Sensor

Sensor in Other Languages

Dutch: **jFlow V5 (Klant specifiek)**, French: **jFlow V5 (personnalisé)**, German: **jFlow V5 (Benutzerdef.)**, Japanese: **jFlow (カスタム)**, Portuguese: **jFlow V5 (customizado)**, Russian: **jFlow**

V5 (нестандартный), Simplified Chinese: jFlow V5 (? ? ?), Spanish: **jFlow V5 (personalizado)**

Remarks

- You have to enable jFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
 - This sensor [does not support more than 50 channels](#)¹²³⁸ officially.
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

JFLOW SPECIFIC SETTINGS

Receive jFlow Packets on UDP Port	<p>Enter the UDP port number on which PRTG receives the flow packets. It must match the one you have configured in the jFlow export options of your hardware router device. Please enter an integer value.</p> <p>i When you configure the export, make sure you select the appropriate jFlow version for this sensor.</p>
Sender IP	Enter the IP address of the sending device you want to receive the jFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

JFLOW SPECIFIC SETTINGS

Receive jFlow Packets on IP	<p>Select the IP address(es) on which PRTG listens to jFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you configured in the jFlow export options of your hardware router device.</p> <p> When you configure the export, make sure you select the appropriate jFlow version for this sensor.</p>
Active Flow Timeout (Minutes)	<p>Enter a time span in minutes after which the sensor must have received new flow data. If the timeout is reached and no new data came in, the sensor may switch to an Unknown status. Please enter an integer value. We recommend you set this one minute longer than the respective timeout configured in your hardware router device.</p> <p> For more details about this setting, see this Knowledge Base article: What is the Active Flow Timeout in Flow sensors?</p> <p> If you set this value too low, flow information might be lost!</p>
Sampling Mode	<p>Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:</p> <ul style="list-style-type: none">▪ Off: The standard flow will be used.▪ On: Switch into sampling mode and specify the sampling rate below.
Sampling Rate	<p>This field is only visible when sampling mode is On above. Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Please enter an integer value.</p>
Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined will be accounted to the default channel named Other.</p> <p> For detailed information, see section Channel Definitions for xFlow and Packet Sniffer Sensors.</p> <p> Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.</p>

JFLOW SPECIFIC SETTINGS

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹²⁴⁷ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹²⁴⁷ below.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[316] settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist

Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplists you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) ³³⁸⁵ on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status** ¹⁹⁵¹. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) ³⁶⁸³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
73 jFlow V5 (Custom) Sensor

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to jFlow V5 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number

More

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

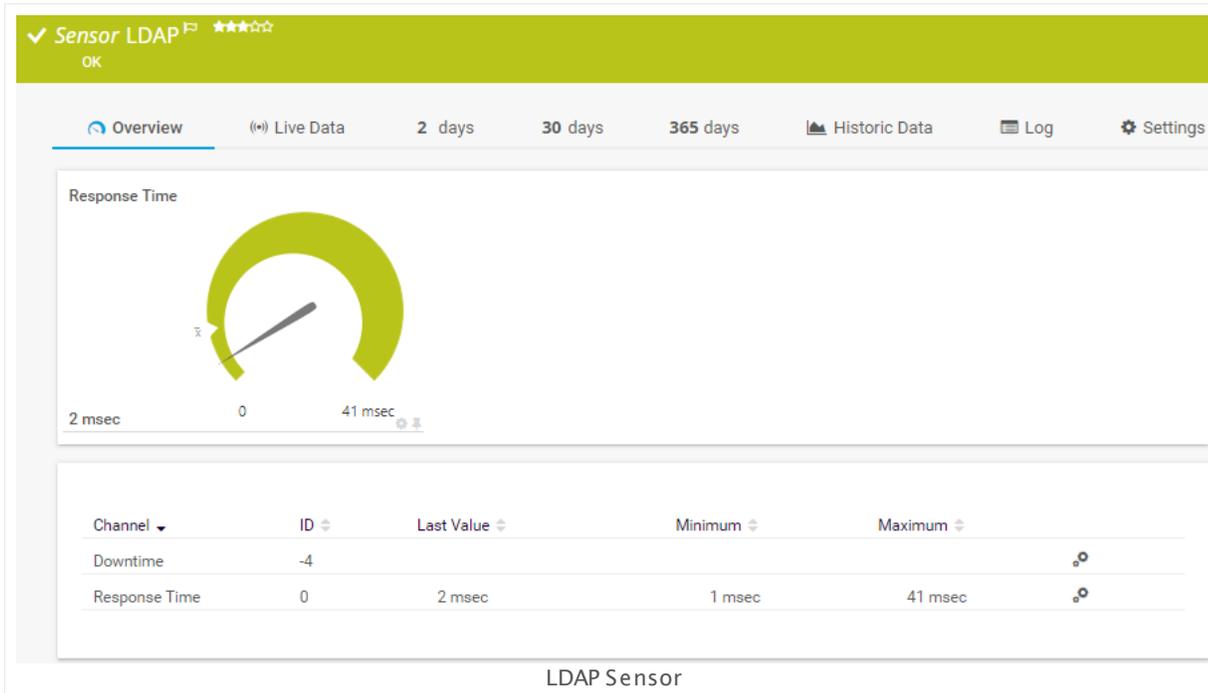
Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.74 LDAP Sensor

The LDAP sensor monitors directory services using Lightweight Directory Access Protocol (LDAP), connecting to the server trying a "bind". If the server does not respond or authentication fails, it will show an error message.

- The sensor shows the response time of the server.



Remarks

- This sensor type does not support LDAP over SSL.
- This sensor type officially supports Microsoft implementations of LDAP. Other third-party LDAP implementations might work but are not officially supported.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

LDAP SPECIFIC

Port	Enter the LDAP port number, usually port 389 for unencrypted connections. Please enter an integer value.
------	--

LDAP SPECIFIC

Distinguished Name	Enter the Distinguished Name (DN) you want to authenticate to the LDAP server. Usually, this is the information for the user you want to authenticate with. For example, use the format cn=Manager,dc=my-domain,dc=com for a DN on an OpenLDAP server.
Password	Enter the password for the entered Distinguished Name .

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <ul style="list-style-type: none"> ❗ To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

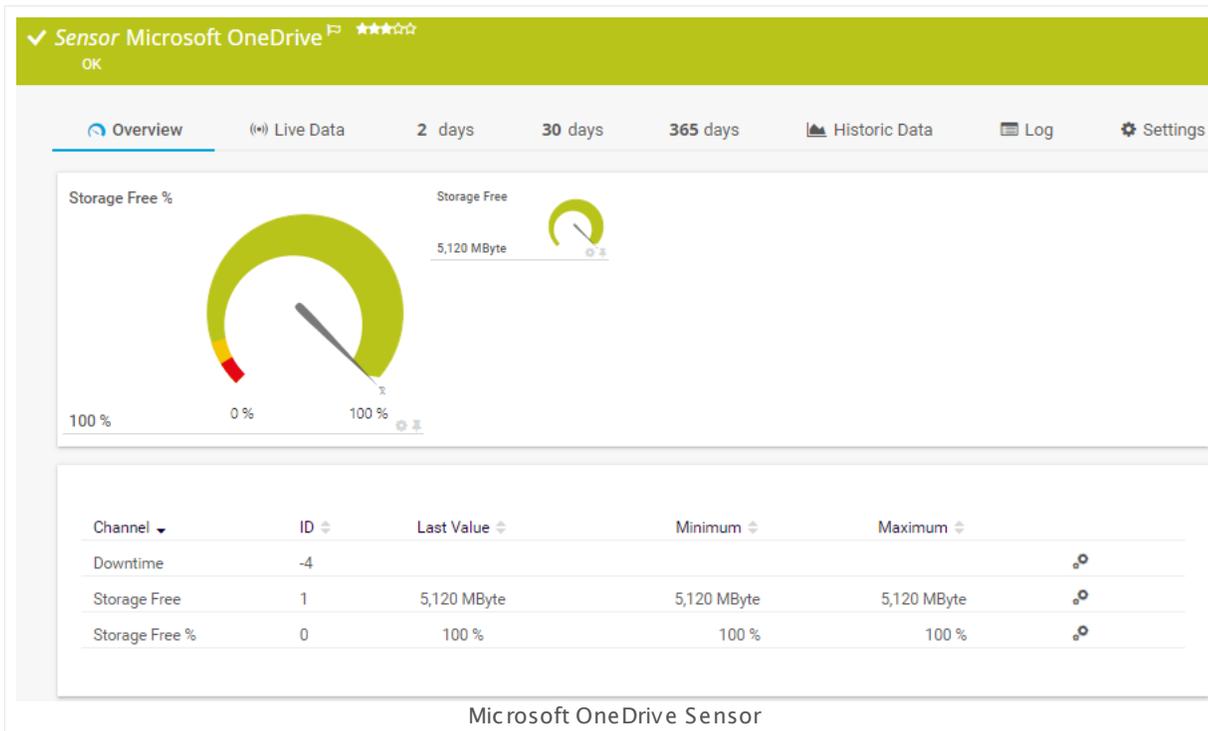
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.75 Microsoft OneDrive Sensor

The Microsoft OneDrive sensor monitors a Microsoft OneDrive Personal account using the OneDrive Application Programming Interface (API) and OAuth2. It shows the following:

- Free storage in bytes and percent



Remarks

- The minimum scanning interval for this sensor type is **30 minutes**.
- For details about OAuth2 authentication, see manual section [Authentication Using OAuth2](#).
- This sensor type only supports OneDrive Personal, it does not work with OneDrive Business.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- PRTG requires OAuth2 authorization before you can actually add this sensor type. Provide the requested credentials in the appearing window.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

MICROSOFT CREDENTIALS

 This sensor type uses **OAuth2** authentication to get access to your Microsoft account. For details about the authentication approach, see section [Authentication Using OAuth2](#)^[1265].

OAuth URL Click the button **Get Access Code** to connect this sensor to your Microsoft account using **OAuth2**. This is necessary to allow the sensor to query data from OneDrive.

A new browser window appears. Please follow the steps there and confirm the permission for PRTG to connect to your OneDrive account. OneDrive forwards you to an empty page after completing the authorization process. Copy the complete **URL** of this empty page and paste it into the **OAuth Code** field below.

OAuth Code Paste the complete **URL** from the address bar of your browser on the empty page to which OneDrive forwards you. The empty page appears after completing the authorization process for PRTG at your OneDrive account. Click **OK** to define the [sensor settings](#)^[935].

 It is mandatory to connect this sensor to your OneDrive account to create this sensor. Please complete the OAuth approach first to get the OAuth code.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

MICROSOFT CREDENTIALS

OAuth Code	Shows the authorization code that the sensor uses to get access to your OneDrive account. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

i This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#) are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Authentication Using OAuth2

 This sensor type uses the OAuth2 security protocol to access the account from which you want to retrieve and monitor data. OAuth2 enables you to grant access to the target account without sharing your password with PRTG. The authorization approach of PRTG using OAuth2 works as follows.

1. Authorization Request

First, you have to request authorization for this sensor to access service resources from your account. For this purpose you are asked to get an access code for this sensor in the **Add Sensor** dialog. Click the **Get Access Code** button to start the authorization process using OAuth2. A new browser window will open on the authorization server of the target service.

2. Verifying Identity

This new window contains a login form for your account that you want to monitor. Log in to your account using your credentials for this service to authenticate your identity. This is a common login to your account on the target server so PRTG will not see your password. The service will forward you to the authorization page and asks you to permit PRTG to access the data in your account.

 If you are already logged in to the service with a user account, you do not have to enter credentials in this step and get directly to the access permission page.

3. Authorizing PRTG

Permit PRTG to access information on your account. Note that this permission holds only for this specific sensor, not for other sensors of this type or PRTG as a whole. For each sensor of this type you add, you have to confirm the access permission anew. You can change the account permissions at any time in your account at the target service.

4. Getting Authorization Code

Permitting PRTG to access your account data forwards you to a page where the service provides an **authorization code**. Copy this code and switch back to the **Add Sensor** dialog in PRTG.

-  The code is only valid a short period of time and expires after a few minutes. You can use a particular code only once.

5. Providing Authorization Code

Paste the authorization code into the **OAuth Code** field and complete the **Add Sensor** dialog. You do not have to go through further configuration steps manually. The sensor will accomplish the following steps automatically.

6. Requesting Access Token

After receiving the authorization code, PRTG will request an access token from the API of the target service. For this purpose, PRTG transmits the authorization code together with several authentication details. The API checks if the authorization is valid and returns the access token to PRTG. Access tokens are specific for one account and one application (here: PRTG). The authorization process to read data from your account is now complete.

7. Retrieving Data

The sensor transmits the access token with each sensor scan in the defined scanning interval to authenticate with your account. It is not necessary to use the original account credentials anew. The used tokens will refresh automatically from time to time.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

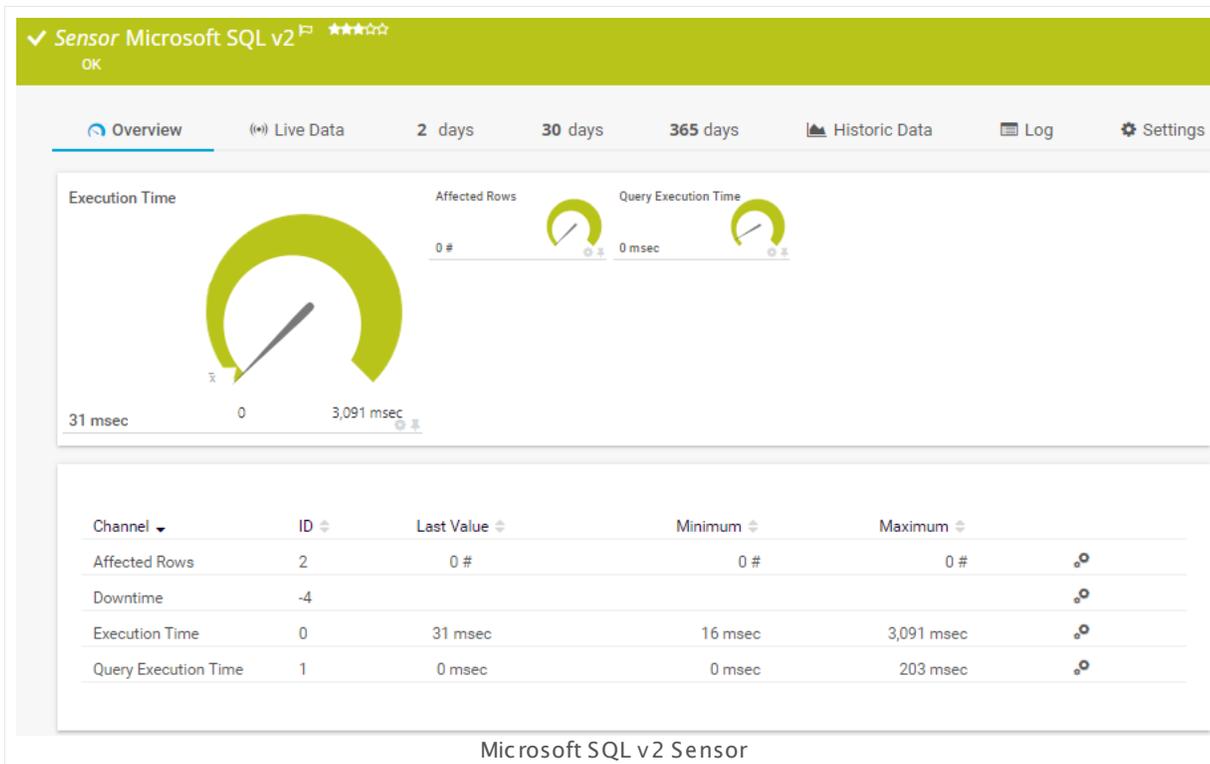
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.76 Microsoft SQL v2 Sensor

The Microsoft SQL v2 sensor monitors a database on a Microsoft SQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of the given query
- Number of rows that were addressed by the query (including **select** statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Remarks

- [Requires](#) ¹²⁶⁰ .NET 4.5 or later on the probe system.
- Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#) ⁴¹³ of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.

- PRTG Manual: [Monitoring Databases](#)^[3534] (includes an [example](#)^[3535] for channel value selection)
 - Knowledge Base: [How to setup the SQL v2 sensors in PRTG? Is there a guide?](#)
 - Knowledge Base: [How can I monitor strings from an SQL database and show a sensor status depending on it?](#)
 - Knowledge Base: [How can I monitor error tables in SQL databases?](#)
 - Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
 - Save the SQL script with the query into the `\Custom Sensors\sql\mssql` subfolder of your PRTG installation. See manual section [Data Storage](#)^[3731] for more information about how to find this path.
 - This sensor type supports Microsoft SQL server 2005 or later.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	Enter the name of the SQL database to which the sensor connects. For example, such a database's name could be MyDatabase . This is a logical entity on the database server where database objects like tables or stored procedures exist.
SQL Server Instance	<p>Define if you want to use an instance name for the database connection. Choose between:</p> <ul style="list-style-type: none"> ▪ No instance name required (default): Use the default instance for the connection. ▪ Use instance name: Use a named instance that you can specify below.

DATABASE SPECIFIC

- Instance Name** This field is only visible if you enable instance name usage above. Enter the named instance you want to monitor.
- Encryption** Define encryption usage for the database connection. Choose between:
- **Use server defaults (default):** The database connection is only encrypted if enforced by the database server.
 - **Enforce encryption but do not validate server certificate:** Choose this option to make sure the database connection is encrypted.
 - **Enforce encryption and validate server certificate:** Choose this option to force encryption and to validate the database server certificate. This approach provides highest security, for example, it helps prevent "man in the middle" attacks.
 The sensor validates the certificate only if the database server enforces encryption!

DATA

- SQL Query File** Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
- The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!
-  For more information on how to find this path, see section [Data Storage](#). By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.
- For example, a correct expression in the file could be: **SELECT AVG (UnitPrice) FROM Products**. If you want to use transactions, separate the individual steps with semicolons ";".
-  Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

DATA

 See also this Knowledge Base article: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

SQL Variables

You can use the following variables in your query file to have them replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: **@prtg**
- Oracle SQL: **:prtg**
- ADO SQL: **?** (question mark)

@prtg, **:prtg**, and **?** behave like common SQL variables, so consider the general rules for SQL variables. For example, you cannot use a variable for a table in the FROM statement of a query.

Example for variables usage: **SELECT * FROM Table WHERE @prtg**

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the variables **@prtg** (Microsoft SQL, MySQL, PostgreSQL), or **:prtg** (Oracle SQL), or **?** (ADO SQL) in the SQL query, considering the general rules for SQL variables. Choose between:

- **Don't use input parameter (default):** Execute the SQL query file without using variables.
- **Use input parameter:** Execute an SQL query file that contains a variable. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter will replace the variable **@prtg** or **:prtg** or **?** in the SQL query, considering the general rules for SQL variables.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, **%sensorid** or **%deviceid**. For details, see section [Custom Sensors](#) ³⁶⁵².

 Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default):** No transactions will be executed.

DATA

- **Use transaction and always rollback:** Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success:** Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Just execute the query:** If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows:** Choose this option if you perform a **SELECT** statement and want to monitor how many rows of the data table this statement returns.
- **Process data table:** Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with **SELECT** statements as well.

Handle DBNull in Channel Values as

This setting is only visible if you select **Process data table** above. Define the sensor behavior if **DBNull** is returned by the query. Choose between:

- **Error:** The sensor will show a **Down** status if **DBNull** is reported.
- **Number 0:** The sensor will recognize the result **DBNull** as a valid value and interpret it as the number **0**.

Select Channel Value by

This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between:

- **Column number:** The channel value will be determined by using the value in row 0 of the column whose number you specify below.
- **Column name:** The channel value will be determined by using the value in row 0 of the column whose name you specify below.
- **Row number:** The channel value will be determined by using the value in column 0 of the row whose number you specify below.

DATA

- **Key value pair:** The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found.

The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below.

 See manual section [Monitoring Databases](#)  for an [example](#)  for channel value selection.

Sensor Channel #x This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for **Channel #1** without enabling it manually. For all other possible channels, choose between:

- **Disable:** This channel will not be added to the sensor.
- **Enable:** This channel will be added to the sensor. Define the settings as described above.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Column Number This setting is only visible if you select **Column number** above. Provide the number of the column that will be used to determine the channel value in row 0. Please enter an integer value.

Sensor Channel #x Column Name This setting is only visible if you select **Column number** above. Provide the name of the column that will be used to determine the channel value in row 0. Please enter a string.

Sensor Channel #x Row Number This setting is only visible if you select **Row number** above. Provide the number of the row that will be used to determine the channel value in column 0. Please enter an integer value.

DATA

Sensor Channel #x Key This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.

Sensor Channel #x Mode This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended):** Shows the value as the sensor retrieves it from the data table.
- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from the data table. This mode is not compatible with the unit **Value Lookup**.

Sensor Channel #x Unit This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#)³⁶⁴².

DATA

 To use [lookups](#) with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x
Value Lookup This settings is only visible if you select **Value Lookup** above. Select a [lookup](#) file that you want to use with this channel.

Use Data Table Value in
Sensor Message This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable:** Do not use a custom sensor message.
- **Enable:** Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

Sensor Message
Column Number This setting is only visible if you select **Column number** and **Use Data Table Value in Sensor Message** above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.

 Columns and rows start with index 0.

Sensor Message
Column Name This setting is only visible if you select **Column name** and **Use Data Table Value in Sensor Message** above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.

 Columns and rows start with index 0.

Sensor Message Row
Number This setting is only visible if you select **Row number** and **Use Data Table Value in Sensor Message** above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.

 Columns and rows start with index 0.

DATA

Sensor Message Key	<p>This setting is only visible if you select Key value pair and Use Data Table Value in Sensor Message above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message	<p>This setting is only visible if you select Use Data Table Value in Sensor Message above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.</p> <p>Example: The message is {0}</p>
If Sensor Message Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification ³¹⁷⁰ whenever the sensor value changes.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- <https://kb.paessler.com/en/topic/18183>

Knowledge Base: How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

PRTG Manual:

- [Monitoring Databases](#)³⁵³⁴

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.77 MySQL v2 Sensor

The MySQL v2 sensor monitors a database on a MySQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows that were addressed by the query (including `select` statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Remarks

- [Requires](#) ^[1268] .NET 4.5 or later on the probe system.
- Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#) ^[413] of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- PRTG Manual: [Monitoring Databases](#) ^[3534] (includes an [example](#) ^[3535] for channel value selection)

- Knowledge Base: [How to setup the SQL v2 sensors in PRTG? Is there a guide?](#)
 - Knowledge Base: [How can I monitor strings from an SQL database and show a sensor status depending on it?](#)
 - Knowledge Base: [How can I monitor error tables in SQL databases?](#)
 - Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
 - Save the SQL script with the query into the `\Custom Sensors\sql\mysql` subfolder of your PRTG installation. See manual section [Data Storage](#)^[373] for more information about how to find this path.
 - This sensor type supports MySQL server version 5.0 or later and might also work with previous versions.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[370]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	<p>Enter the name of the MySQL database to which the sensor connects. For example, such a database's name could be MyDatabase. This is a logical entity on the database server where database objects like tables or stored procedures exist.</p> <p>The database name of a MySQL server also reflects a physical directory structure where your database objects are stored. Enter the appropriate string, which is the same as you would supply when invoking the mysql.exe admin tool (with the command line switch -p) or after the login with mysql.exe with the command use.</p>
----------	---

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific `\Custom Sensors\sql` subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

 For more information on how to find this path, see section [Data Storage](#). By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: **SELECT AVG (UnitPrice) FROM Products**. If you want to use transactions, separate the individual steps with semicolons ";".

 Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

 See also this Knowledge Base article: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

SQL Variables

You can use the following variables in your query file to have them replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: **@prt g**
- Oracle SQL: **:prt g**
- ADO SQL: **?** (question mark)

@prt g, **:prt g**, and **?** behave like common SQL variables, so consider the general rules for SQL variables. For example, you cannot use a variable for a table in the FROM statement of a query.

Example for variables usage: **SELECT * FROM Table WHERE @prt g**

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the variables **@prt g** (Microsoft SQL, MySQL, PostgreSQL), or **:prt g** (Oracle SQL), or **?** (ADO SQL) in the SQL query, considering the general rules for SQL variables. Choose between:

DATA

- **Don't use input parameter (default):** Execute the SQL query file without using variables.
- **Use input parameter:** Execute an SQL query file that contains a variable. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter will replace the variable `@prtg` or `:prtg` or `?` in the SQL query, considering the general rules for SQL variables.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, `%sensorid` or `%deviceid`. For details, see section [Custom Sensors](#).

 Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default):** No transactions will be executed.
- **Use transaction and always rollback:** Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success:** Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Just execute the query:** If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows:** Choose this option if you perform a **SELECT** statement and want to monitor how many rows of the data table this statement returns.

DATA

- **Process data table:** Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with **SELECT** statements as well.

Handle DBNull in Channel Values as

This setting is only visible if you select **Process data table** above. Define the sensor behavior if **DBNull** is returned by the query. Choose between:

- **Error:** The sensor will show a **Down** status if **DBNull** is reported.
- **Number 0:** The sensor will recognize the result **DBNull** as a valid value and interpret it as the number **0**.

Select Channel Value by

This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between:

- **Column number:** The channel value will be determined by using the value in row 0 of the column whose number you specify below.
- **Column name:** The channel value will be determined by using the value in row 0 of the column whose name you specify below.
- **Row number:** The channel value will be determined by using the value in column 0 of the row whose number you specify below.
- **Key value pair:** The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found.

The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below.

 See manual section [Monitoring Databases](#)  for an [example](#)  for channel value selection.

Sensor Channel #x

This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for **Channel #1** without enabling it manually. For all other possible channels, choose between:

- **Disable:** This channel will not be added to the sensor.
- **Enable:** This channel will be added to the sensor. Define the settings as described above.

DATA

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Column Number This setting is only visible if you select **Column number** above. Provide the number of the column that will be used to determine the channel value in row 0. Please enter an integer value.

Sensor Channel #x Column Name This setting is only visible if you select **Column number** above. Provide the name of the column that will be used to determine the channel value in row 0. Please enter a string.

Sensor Channel #x Row Number This setting is only visible if you select **Row number** above. Provide the number of the row that will be used to determine the channel value in column 0. Please enter an integer value.

Sensor Channel #x Key This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.

Sensor Channel #x Mode This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended):** Shows the value as the sensor retrieves it from the data table.
- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from the data table. This mode is not compatible with the unit **Value Lookup**.

Sensor Channel #x Unit This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth

DATA

- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#).

 To use [lookups](#) with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x
Value Lookup

This settings is only visible if you select **Value Lookup** above. Select a [lookup](#) file that you want to use with this channel.

Use Data Table Value in
Sensor Message

This setting is only visible if you select **Process data table** above. Define if the sensor message will show a value from the data table. Choose between:

- **Disable**: Do not use a custom sensor message.
- **Enable**: Define a custom sensor message with a defined value of the data table. Define the value selection below.

The method to determine a value for the sensor message is defined in setting **Select Channel Value by** above.

DATA

Sensor Message Column Number	<p>This setting is only visible if you select Column number and Use Data Table Value in Sensor Message above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Column Name	<p>This setting is only visible if you select Column name and Use Data Table Value in Sensor Message above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Row Number	<p>This setting is only visible if you select Row number and Use Data Table Value in Sensor Message above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Key	<p>This setting is only visible if you select Key value pair and Use Data Table Value in Sensor Message above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message	<p>This setting is only visible if you select Use Data Table Value in Sensor Message above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.</p> <p>Example: The message is {0}</p>
If Sensor Message Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none">▪ Ignore changes (default): The sensor takes no action on change.▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>3170</small> whenever the sensor value changes.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p>

DATA

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- <https://kb.paessler.com/en/topic/18183>

Knowledge Base: How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

PRTG Manual:

- [Monitoring Databases](#)³⁵³⁴

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.78 NetApp Aggregate Sensor

The NetApp Aggregate sensor monitors the status of a NetApp cDOT or ONTAP storage aggregate accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Number of files on the aggregate
- Number of disks on the aggregate
- Status of the aggregate (online, restrict, offline, other error)
- Read and written blocks per second
- User reads and writes per seconds
- Free bytes in total and percent

✓ Sensor NetApp Aggregate ☆☆☆☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Files

96 #

Aggregate State	Online	Blocks read	10.143413587895...	Blocks written	47.528185409709...	Bytes Free	157,482 MByte
Bytes Free %	98 %	Data read	0.28 MByte/s	Data written	0.19 MByte/s	Disks #	55 #
Latency	55 msec	User reads	1.5308191966394...	User writes	6.7828348215526 ...		

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	⚙
Aggregate State	9	Online		Online	Online	⚙
Blocks read	5	18255 #	10.1434135878957...	5.35744182153022...	28.5615083774054...	⚙
Blocks written	6	85536 #	47.5281854097095...	34.6894357944082...	52.0170901231756...	⚙
Bytes Free	3	157,482 MByte		157,432 MByte	157,482 MByte	⚙
Bytes Free %	4	98 %		98 %	98 %	⚙
Data read	12	502 MByte	0.28 MByte/s	0.19 MByte/s	0.37 MByte/s	⚙
Data written	11	334 MByte	0.19 MByte/s	0.14 MByte/s	0.20 MByte/s	⚙
Disks #	10	55 #		55 #	55 #	⚙
Downtime	-4					⚙
Files	2	96 #		96 #	96 #	⚙
Latency	13	55 msec		40 msec	327 msec	⚙
User reads	7	2755 #	1.53081919663942...	0.53574418215302...	13.3538509399582...	⚙
User writes	8	12207 #	6.7828348215526 ...	5.39095566941412...	6.95399553397843...	⚙

NetApp Aggregate Sensor

1300

8/14/2018

Sensor in Other Languages

Dutch: **NetApp Aggregate**, French: **Agrégat NetApp**, German: **NetApp Aggregat**, Japanese: **NetApp? ? ?**, Portuguese: **NetApp Aggregate**, Russian: **Статистическое выражение NetApp**, Simplified Chinese: **NetApp? ?**, Spanish: **Agregado de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#)¹³⁰² to **ONTAPI (DATA ONTAP API)** so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: Net App System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type supersedes the deprecated NetApp cDOT Aggregate (SOAP) sensor.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the **local system** (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

🧠 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the aggregates that you want to monitor. PRTG will create one sensor for each aggregate you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp Aggregates	Select all aggregates that you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-------------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none"> ▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor. ▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
--------------------	--

NETAPP CONNECTION

Username	This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.
Password	This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.
Port	Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443 .
Transport Type	Define if the connection to the NetApp API is TLS/SSL secured. Choose between: <ul style="list-style-type: none">▪ HTTP: Use an unsecured HTTP connection.▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP SPECIFIC

NetApp Aggregates	Shows the aggregate that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------------	---

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	---

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

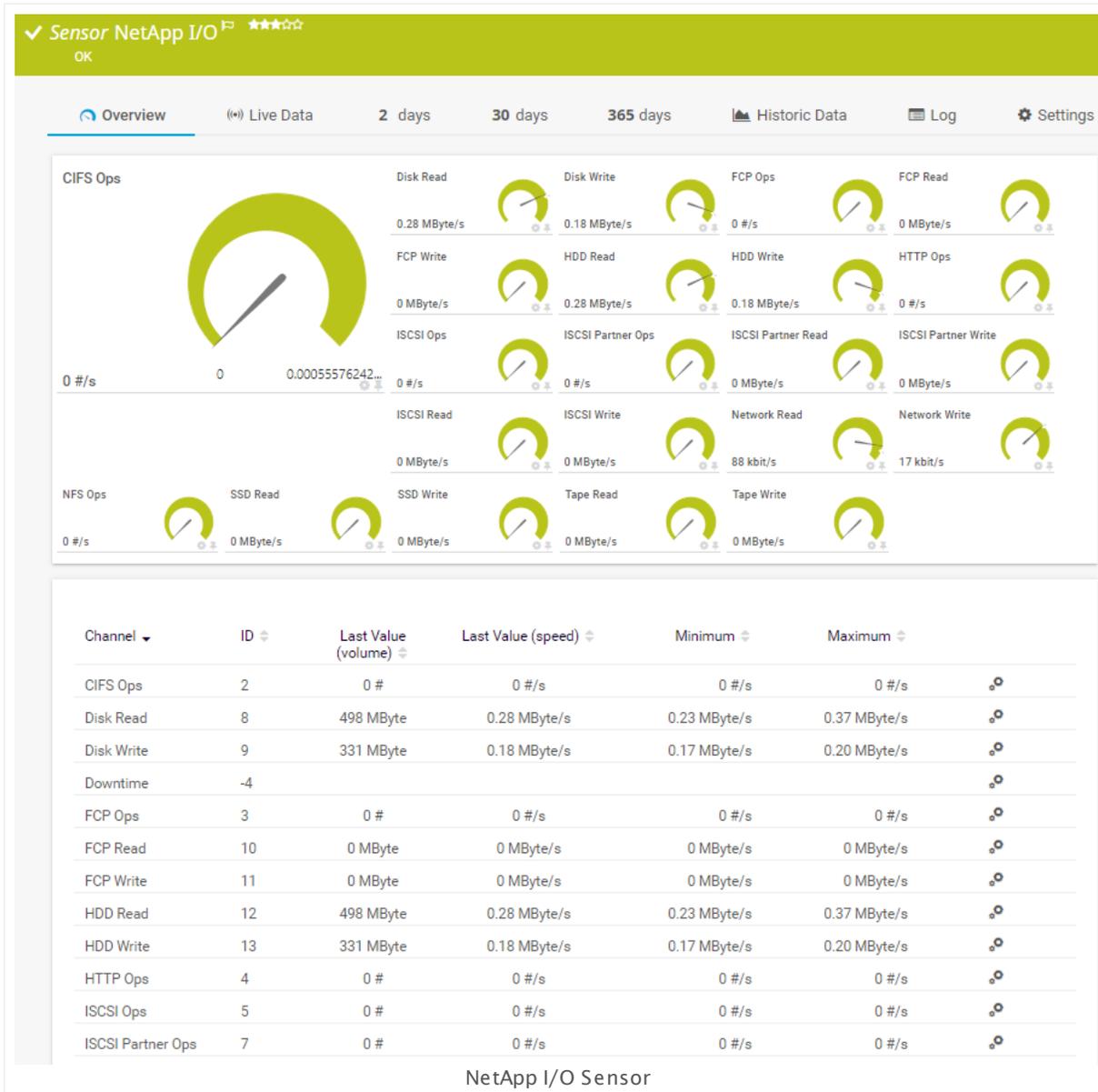
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.79 NetApp I/O Sensor

The NetApp I/O sensor monitors input and output operations of a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Number of Common Internet File System (CIFS) operations per second
- Disk read and write speed
- Number of FCP operations per second
- FCP read and write speed
- HDD read and write speed
- HTTP operations per second
- Number of internet Small Computer System Interface (iSCSI) operations per second
- iSCSI read and write speed
- Number of iSCSI partner operations per second
- iSCSI partner read and write speed
- Network read and write speed
- Number of Network File System (NFS) operations per second
- SSD read and write speed
- Tape read and write speed

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
79 NetApp I/O Sensor



Sensor in Other Languages

Dutch: **NetApp I/O**, French: **E/S NetApp**, German: **Net App I/O**, Japanese: **NetApp I/O**, Portuguese: **NetApp E/S**, Russian: **Ввод-вывод NetApp**, Simplified Chinese: **NetApp I/O**, Spanish: **E/S de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#) to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.

- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: Net App System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type supersedes the deprecated NetApp cDOT I/O (SOAP) sensor.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the system nodes that you want to monitor. PRTG will create one sensor for each node you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp System Nodes Select all nodes that you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials Specify which credentials you want to use to connect to the NetApp API. Choose between:

- **Use explicit credentials:** Choose this option if you want to use individual NetApp API credentials with this sensor.
- **Use Windows credentials from parent device:** If you choose this option, the sensor will use the credentials (**User and Password**) that you enter in the [parent device settings](#)^[407] in section **Credentials for Windows Systems**. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.

Username This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.

Password This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.

Port Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is **443**.

Transport Type Define if the connection to the NetApp API is TLS/SSL secured. Choose between:

- **HTTP:** Use an unsecured HTTP connection.
- **HTTPS:** Use a TLS/SSL secured connection to the defined port to send the query.

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

NETAPP SPECIFIC

NetApp System Nodes Shows the ID of the system node that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

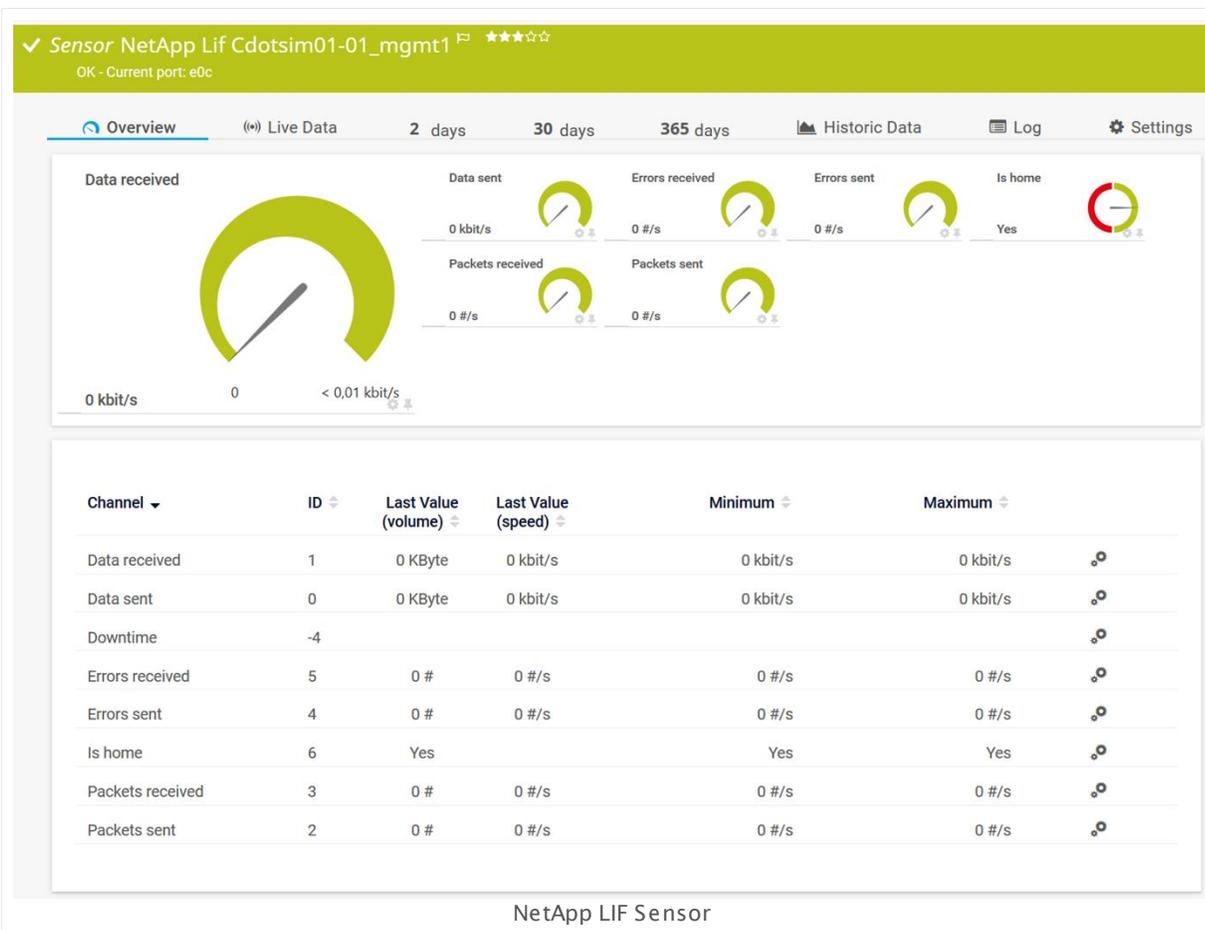
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.80 NetApp LIF Sensor

The NetApp LIF sensor monitors logical interfaces of a NetApp cDOT or ONTAP cluster accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP).

It shows the following:

- Number of sent and received packets per second
- Amount of sent and received data per second
- Number of sent and received errors per second
- Is home: **up status** when LIF is on the home port, **down** status when it is not on the home port



Sensor in Other Languages

Dutch: **NetApp LIF**, French: **LIF NetApp**, German: **NetApp LIF**, Japanese: **NetApp LIF**, Portuguese: **NetApp LIF**, Russian: **LIF NetApp**, Simplified Chinese: **NetApp LIF**, Spanish: **LIF de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#)¹³⁰² to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: Net App System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the logical interfaces that you want to monitor. PRTG will create one sensor for each LIF you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp LIFs

Select the logical interfaces you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none"> ▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor. ▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
Username	This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.
Password	This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.

NETAPP CONNECTION

Port	Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443 .
Transport Type	Define if the connection to the NetApp API is TLS/SSL secured. Choose between: <ul style="list-style-type: none">▪ HTTP: Use an unsecured HTTP connection.▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP SPECIFIC

NetApp LIFs	Shows the ID of the logical interface that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------	---

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.<ul style="list-style-type: none">📖 For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. <p>☁ This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

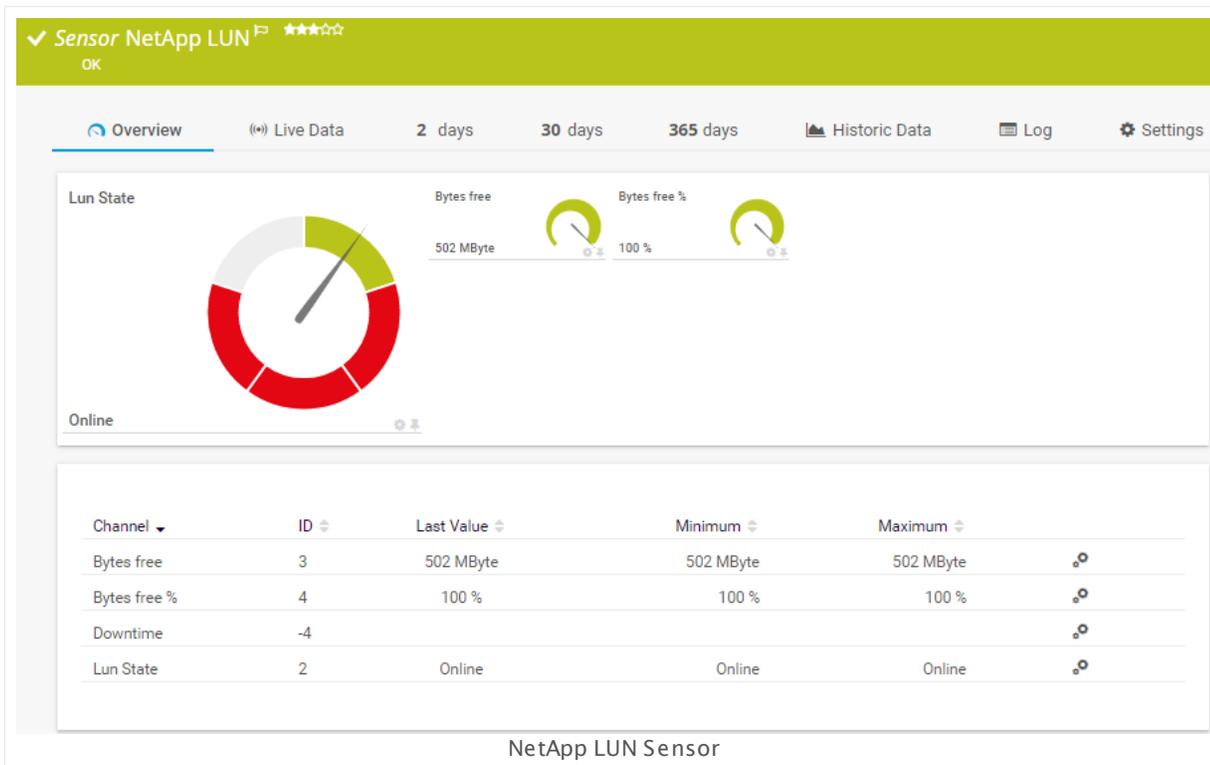
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.81 NetApp LUN Sensor

The NetApp LUN sensor monitors the logical unit number (LUN) of a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Status of the LUN:
 - Online
 - Offline due to a media error on the associated foreign LUN
 - Offline due to an NVRAM failure
 - Offline due to insufficient space
 - Administratively offline or unknown reason
- Free bytes in percent and total
- Read and write operations per second
- Read and write blocks per second
- Other operations per second
- Number of SCSI errors per second
- Mapping status of the LUN (mapped: yes or no)



Sensor in Other Languages

Dutch: **NetApp LUN**, French: **LUN NetApp**, German: **NetApp LUN**, Japanese: **NetApp LUN**, Portuguese: **NetApp LUN**, Russian: **LUN NetApp**, Simplified Chinese: **NetApp LUN**, Spanish: **LUN de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#)¹³⁰² to **ONTAPI** (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster** | **ClusterX** | **Configuration** | **Security** | **Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: NetApp System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the LUNs that you want to monitor. PRTG will create one sensor for each LUN you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp LUNs

Select the LUNs you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none"> ▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor. ▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings^[407] in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
--------------------	--

NETAPP CONNECTION

Username	This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.
Password	This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.
Port	Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443 .
Transport Type	Define if the connection to the NetApp API is TLS/SSL secured. Choose between: <ul style="list-style-type: none">▪ HTTP: Use an unsecured HTTP connection.▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP SPECIFIC

NetApp LUNs	Shows the ID of the LUN that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------	---

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	---

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.82 NetApp NIC Sensor

The NetApp NIC sensor monitors the network interface controller (NIC) of a NetApp cDOT or ONTAP cluster accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Sent and received bytes per second
- Number of sent and received errors per second
- Number of up to down links per seconds



Sensor in Other Languages

Dutch: **NetApp NIC**, French: **NIC NetApp**, German: **NetApp NIC**, Japanese: **NetApp NIC**, Portuguese: **NetApp NIC**, Russian: **NIC NetApp**, Simplified Chinese: **NetApp NIC**, Spanish: **NIC de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#) ¹³⁰² to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.

- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: Net App System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the network interface controllers that you want to monitor. PRTG will create one sensor for each NIC you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp NICs Select the NICs you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) [402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) [181], as well as in [alarms](#) [219], [logs](#) [228], [notifications](#) [3216], [reports](#) [3252], [maps](#) [3276], [libraries](#) [3235], and [tickets](#) [230].

Parent Tags Shows [Tags](#) [139] that this sensor [inherits](#) [140] from its [parent device, group, and probe](#) [133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) [139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) [140] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	Specify which credentials you want to use to connect to the NetApp API. Choose between: <ul style="list-style-type: none"> ▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor. ▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings^[407] in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
Username	This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.
Password	This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.
Port	Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443 .
Transport Type	Define if the connection to the NetApp API is TLS/SSL secured. Choose between: <ul style="list-style-type: none"> ▪ HTTP: Use an unsecured HTTP connection. ▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.

NETAPP CONNECTION

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

NETAPP SPECIFIC

NetApp NICs Shows the ID of the NIC that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

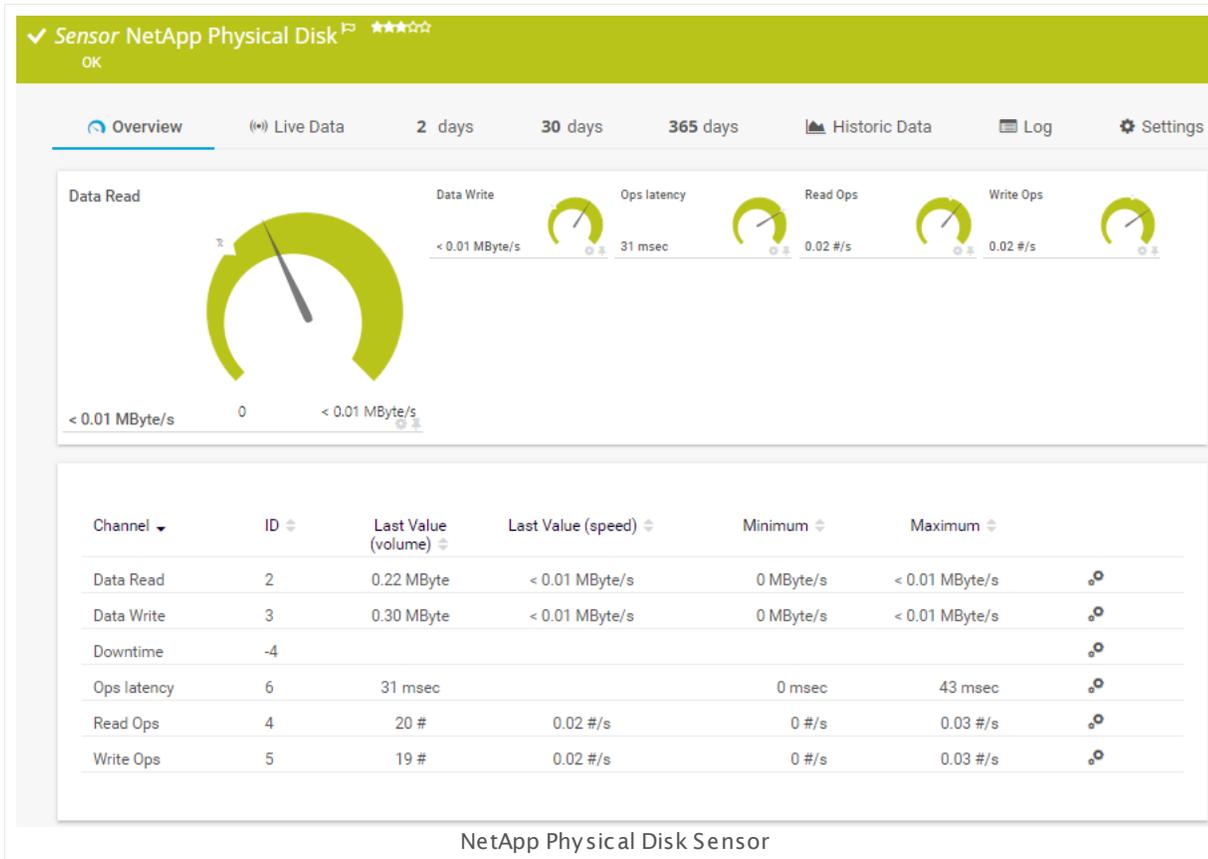
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.83 NetApp Physical Disk Sensor

The NetApp Physical Disk sensor monitors disks of a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Latency of operations
- Read and write speed of operations
- Data read and write speed



Sensor in Other Languages

Dutch: **NetApp cDOT Fysieke Schijf**, French: **Disque physique NetApp**, German: **NetApp Physikal. Laufwerk**, Japanese: **NetApp? ? ? ? ?**, Portuguese: **NetApp Disco físico**, Russian: **Физический диск NetApp**, Simplified Chinese: **NetApp? ? ? ?**, Spanish: **Disco físico de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#) to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.

- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: Net App System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type supersedes the deprecated NetApp cDOT Physical Disk (SOAP) sensor.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the disks you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp Disk Select all disks that you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none">▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor.▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings^[407] in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
Username	<p>This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.</p>
Password	<p>This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443.</p>
Transport Type	<p>Define if the connection to the NetApp API is TLS/SSL secured. Choose between:</p> <ul style="list-style-type: none">▪ HTTP: Use an unsecured HTTP connection.▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

NETAPP SPECIFIC

NetApp Disk Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
83 NetApp Physical Disk Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

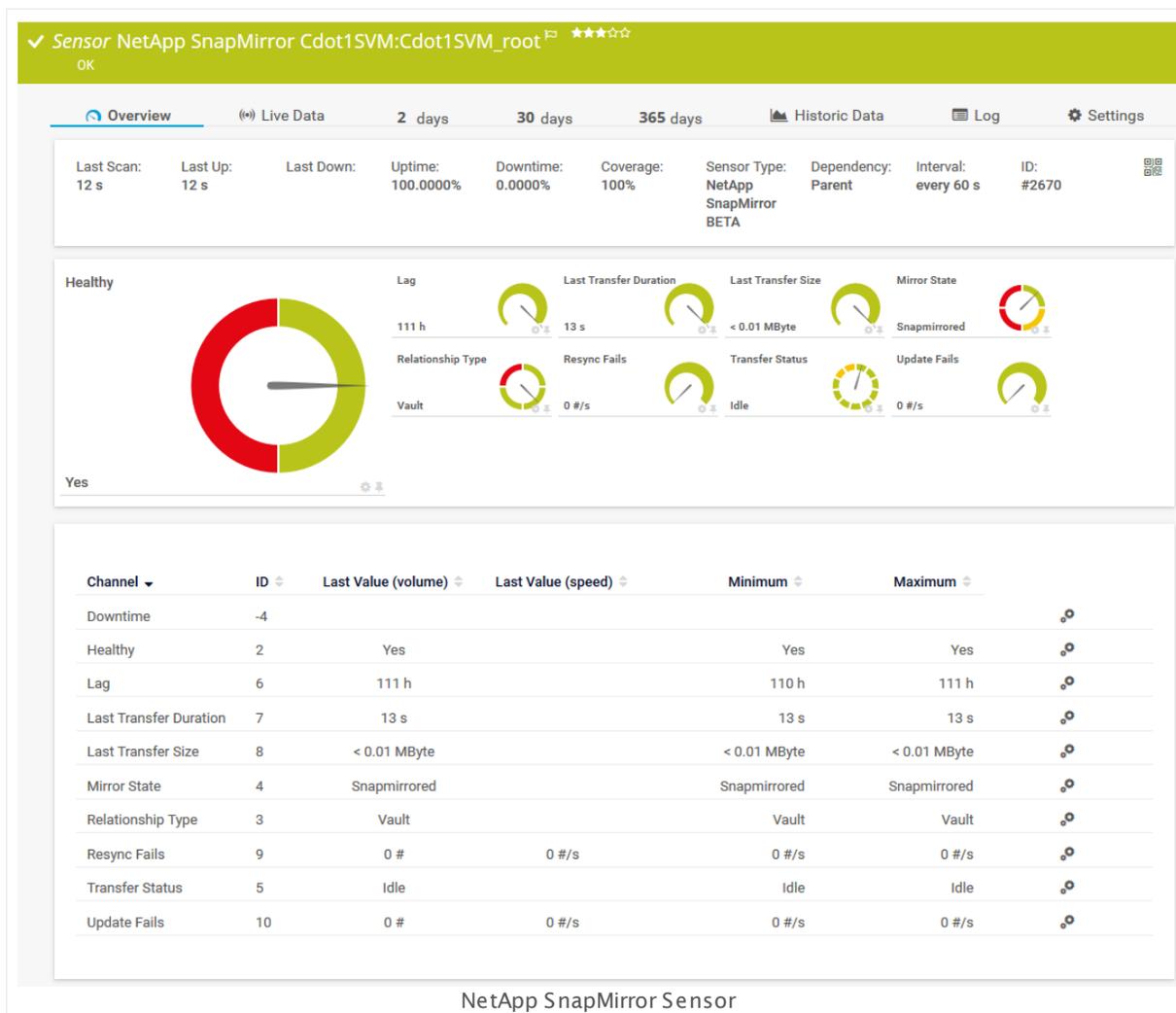
7.8.84 NetApp SnapMirror Sensor

The NetApp SnapMirror sensor monitors SnapMirror relationships of a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Health status (healthy **yes** or **no**)
- Transfer status (relationship status returned from the API)
 - **Ok**: idle, transferring, checking, quiescing, quiesced, queued, preparing, finalizing, aborting
 - **Warning**: unknown, breaking
- Lag transfer duration
- Relationship type
 - **Ok**: mirror, vault, mirror and vault
 - **Error**: unknown
- Size of last transfer
- Duration of last transfer
- Timestamp of last transfer
- Number of resync fails per second
- Number of update fails per second
- Mirror state
 - **Ok**: snapmirrored
 - **Warning**: uninitialized
 - **Error**: broken-off, unknown

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

84 NetApp SnapMirror Sensor



Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#)^[1302] to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**
- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: NetApp System Health Sensor—Permissions: Alternative to Admin Rights](#)^[1381]
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)^[407] in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clustered -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the SnapMirrors you want to monitor. PRTG will create one sensor for each SnapMirror you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp SnapMirrors Select all SnapMirrors that you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none">▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor.▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings^[407] in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
Username	<p>This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.</p>
Password	<p>This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.</p>
Port	<p>Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443.</p>
Transport Type	<p>Define if the connection to the NetApp API is TLS/SSL secured. Choose between:</p> <ul style="list-style-type: none">▪ HTTP: Use an unsecured HTTP connection.▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>

NETAPP SPECIFIC

NetApp SnapMirrors Shows the SnapMirror that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

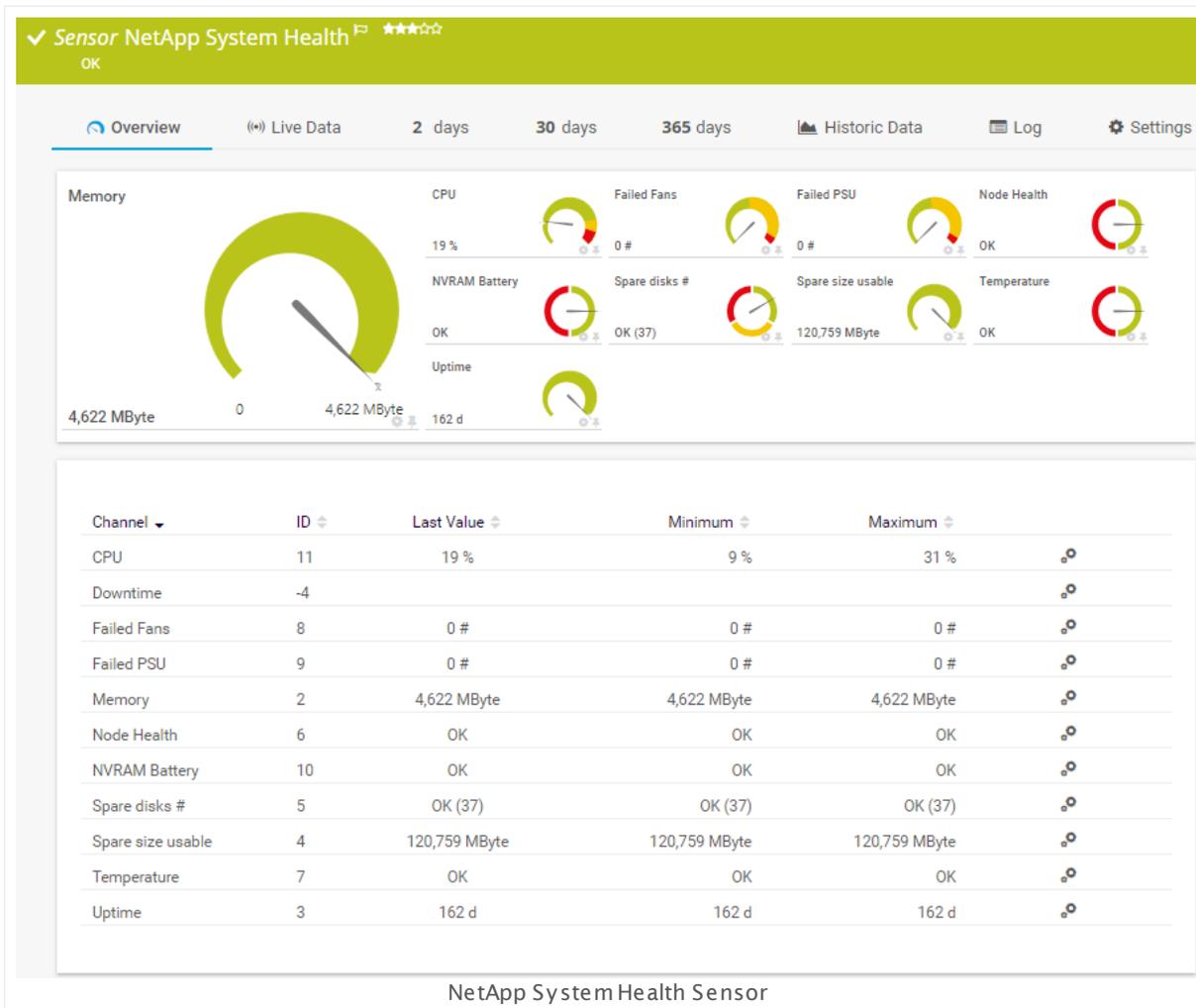
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.85 NetApp System Health Sensor

The NetApp System Health sensor monitors the health of a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Memory usage
 - CPU load
 - Uptime
 - Number of failed fans
 - Number of failed PSU
 - Node health (error or OK)
 - NVRAM battery status (error or OK)
 - Number of spare disks
 - Low spare disks as reported by the NetApp (yes or no)
 - Usable spare size
 - Temperature status (error or OK)
 - Storage configuration path, which describes the connection of a node
 - **Up** [status](#)¹⁹⁵: multi_path, multi_path_ha, N/A
 - **Warning** status: single_path, single_path_ha, mixed_path, mixed_path_ha
 - **Down** status: unknown
- i** If there is no storage configuration path returned, the sensor will show an up status (N/A) because the availability of the configuration path depends on the NetApp version.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 85 NetApp System Health Sensor



NetApp System Health Sensor

Sensor in Other Languages

Dutch: **NetApp Systeem Gesteldheid**, French: **État du système NetApp**, German: **NetApp Systemzustand**, Japanese: **NetApp ? ? ? ? ? ?** , Portuguese: **NetApp Funcionamento do sistema**, Russian: **Работоспособность системы NetApp**, Simplified Chinese: **NetApp ? ? ? ? ? ?** , Spanish: **Estado del sistema de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#) ¹³⁰² to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**

- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: NetApp System Health Sensor—Permissions: Alternative to Admin Rights](#)¹³⁸¹
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)⁴⁰⁷ in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- This sensor type supersedes the deprecated NetApp cDOT System Health (SOAP) sensor.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the **local** system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Permissions: Alternative to Admin Rights

If you do not want to provide admin rights for the ONTAPI user account that you use with the NetApp System Health sensor, you can add a new command to the selected role of the user that makes read-only rights sufficient.

- Edit the **Role** of this user in the console under **Cluster | ClusterX | Configuration | Security | Users**.
- **Add** the command **storage aggregate check_spare_low** with ACL **all** to the **Role Attributes**.
- ✓ With this role attribute, read-only rights are sufficient for the NetApp System Health sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the system nodes that you want to monitor. PRTG will create one sensor for each node you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp System Nodes Select the nodes you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) ¹⁸¹, as well as in [alarms](#) ²¹⁹, [logs](#) ²²⁸, [notifications](#) ³²¹⁶, [reports](#) ³²⁵², [maps](#) ³²⁷⁸, [libraries](#) ³²³⁵, and [tickets](#) ²³⁰.

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials	<p>Specify which credentials you want to use to connect to the NetApp API. Choose between:</p> <ul style="list-style-type: none"> ▪ Use explicit credentials: Choose this option if you want to use individual NetApp API credentials with this sensor. ▪ Use Windows credentials from parent device: If you choose this option, the sensor will use the credentials (User and Password) that you enter in the parent device settings in section Credentials for Windows Systems. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.
Username	This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.
Password	This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.

NETAPP CONNECTION

Port	Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is 443 .
Transport Type	Define if the connection to the NetApp API is TLS/SSL secured. Choose between: <ul style="list-style-type: none"> ▪ HTTP: Use an unsecured HTTP connection. ▪ HTTPS: Use a TLS/SSL secured connection to the defined port to send the query.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

NETAPP SPECIFIC

NetApp System Nodes	Shows the ID of the system node that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
---------------------	---

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> ▪  For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. ▪  This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.
---------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

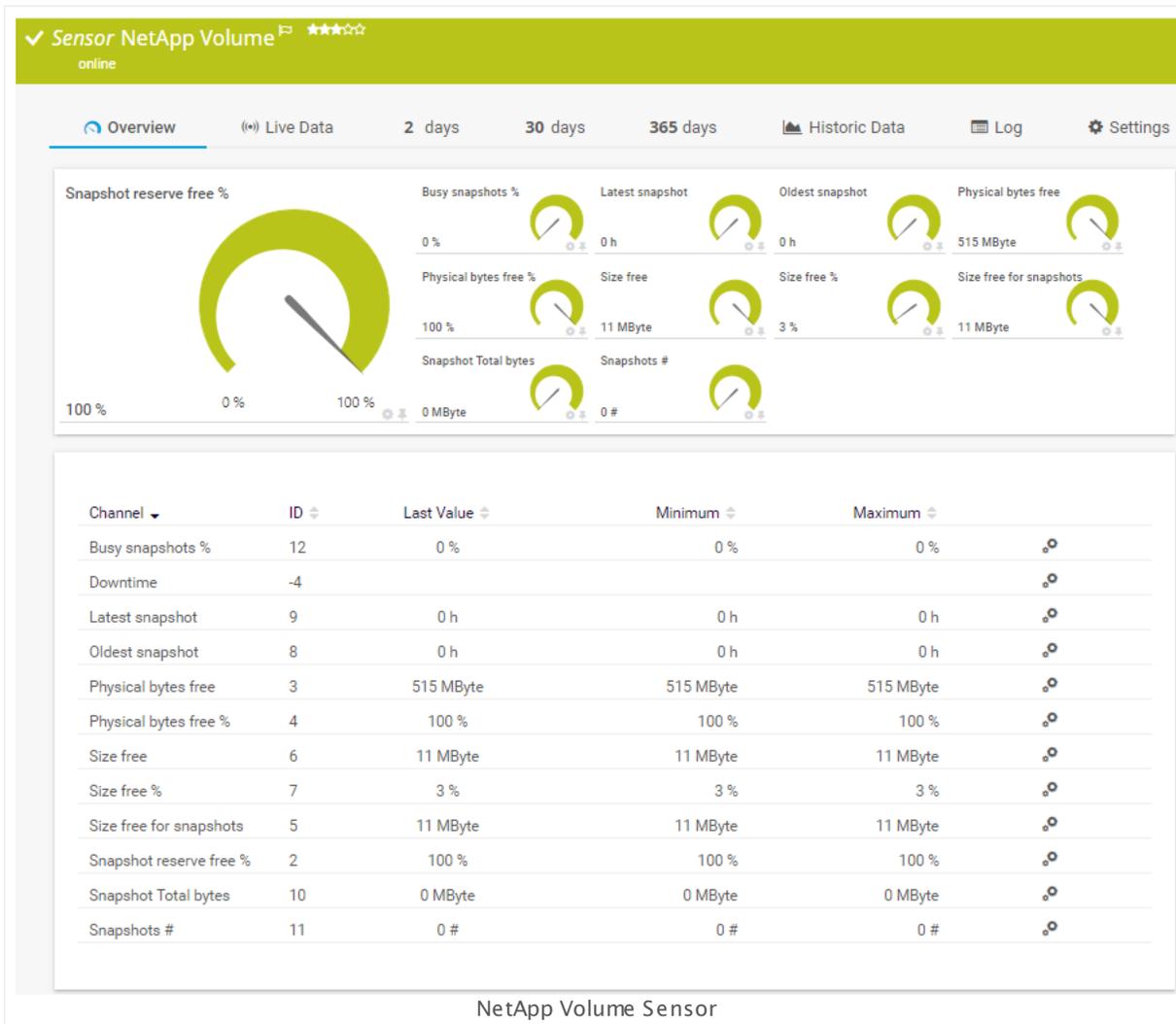
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.86 NetApp Volume Sensor

The NetApp Volume sensor monitors volumes on a NetApp cDOT or ONTAP storage system accessing the Application Programming Interface (API) via Simple Object Access Protocol (SOAP). It can show the following:

- Free space for snapshots in percent and total
- Busy snapshots in percent
- Age of latest snapshot
- Age of oldest snapshot
- Total bytes of snapshots
- Number of snapshots
- Free physical bytes in percent and total
- Free size in percent and total
- Free files in percent and total
- Compression savings in percent and total
- Deduplication savings in percent and total
- Total savings in percent and total

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
86 NetApp Volume Sensor



NetApp Volume Sensor

Sensor in Other Languages

Dutch: **NetApp Volume**, French: **Volume NetApp**, German: **NetApp Volume**, Japanese: **NetApp? ? ? ? ?**, Portuguese: **NetApp Volume**, Russian: **Tom NetApp**, Simplified Chinese: **NetApp ?**, Spanish: **Volumen de NetApp**

Remarks

- This sensor type supports the NetApp cDOT 8.3 and NetApp ONTAP 9.0 or later.
- The ONTAPI user account that you use with this sensor needs [access](#) to ONTAPI (DATA ONTAP API) so that the sensor can request data from it. The access is enabled by default.
- The NetApp System Health sensor requires **admin** permissions for the ONTAPI user account that you use to access ONTAPI. For other NetApp sensors, read-only user rights are sufficient. Modify or add this user with a suitable role in the console under **Cluster | ClusterX | Configuration | Security | Users**

- As alternative to admin permissions for the NetApp System Health sensor, you can add a specific **Role Attribute** and use read-only rights. For details, see [PRTG Manual: NetApp System Health Sensor—Permissions: Alternative to Admin Rights](#)^[1381]
- You can define NetApp API credentials (**User** and **Password**) in the [parent device settings](#)^[407] in section **Credentials for Windows Systems**. This way, you will not have to individually enter credentials for each NetApp sensor that you add to the same device.
- Requires .NET 4.5 on the probe system.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Requirement: .NET Framework

✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

💡 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Enabled ONTAPI Access

NetApp sensors require access to ONTAPI for the utilized user account, which is enabled by default. If access is disabled, use the following command locally on the cluster console to enable ONTAPI access for the user:

```
services web> modify -vserver clusterd -name ontapi -enabled true
```

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the volumes that you want to monitor. PRTG will create one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

NETAPP SPECIFIC

NetApp Volumes Select the volumes you want to add a sensor to. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 Volumes that are offline will not appear in this list.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP CONNECTION

NetApp Credentials Specify which credentials you want to use to connect to the NetApp API. Choose between:

- **Use explicit credentials:** Choose this option if you want to use individual NetApp API credentials with this sensor.
- **Use Windows credentials from parent device:** If you choose this option, the sensor will use the credentials (**User and Password**) that you enter in the [parent device settings](#)^[407] in section **Credentials for Windows Systems**. Defining credentials in the parent device is useful if you add several NetApp sensors to this device because you will not have to individually enter credentials for each NetApp sensor.

Username This field is only available if you select explicit credentials above. Enter a username for access to the NetApp API. Read-only rights for this ONTAP user account are sufficient. Please enter a string.

Password This field is only available if you select explicit credentials above. Enter the password of the user that you entered above for access to the NetApp API. Please enter a string.

Port Enter a port number on which you can access the NetApp API. Please enter an integer value. The default port is **443**.

Transport Type Define if the connection to the NetApp API is TLS/SSL secured. Choose between:

- **HTTP:** Use an unsecured HTTP connection.
- **HTTPS:** Use a TLS/SSL secured connection to the defined port to send the query.

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

NETAPP SPECIFIC

NetApp Volumes Shows the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁️ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
86 NetApp Volume Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.87 NetFlow V5 Sensor

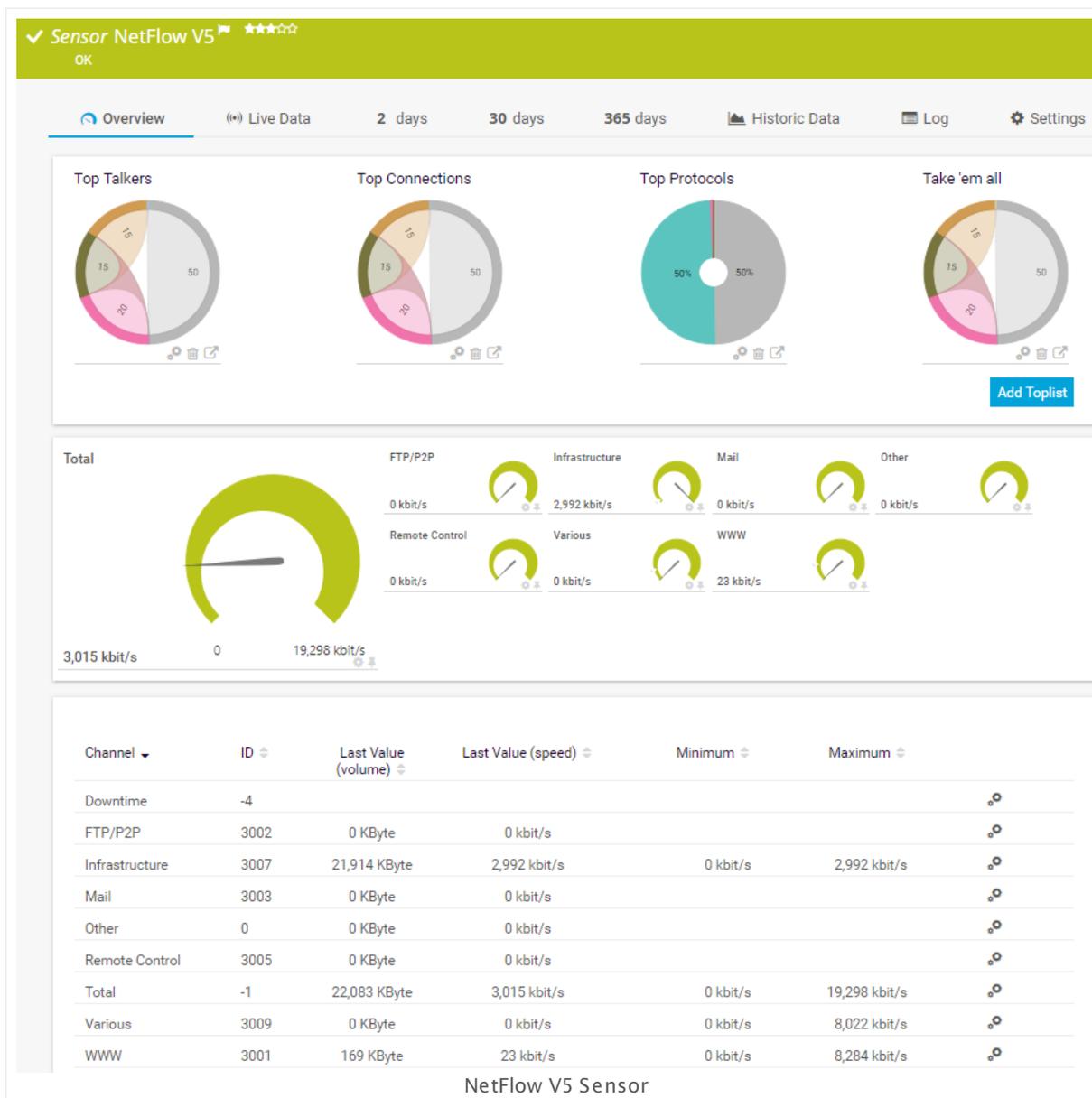
The NetFlow V5 sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Ensure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
87 NetFlow V5 Sensor



Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)
- Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)

- For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#).

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value.

 When configuring export, make sure you select the appropriate NetFlow version for this sensor.

Sender IP Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

Receive NetFlow Packets on IP Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address selected here must match the one you have configured in the NetFlow export options of your hardware router device.

 When configuring export, make sure you select the appropriate NetFlow version for this sensor.

Active Flow Timeout (Minutes) Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown status**¹⁹⁵. Please enter an integer value.

We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

 If you set this value too low, flow information might be lost!

 For more details, see this Knowledge Base article: [What is the Active Flow Timeout in Flow sensors?](#)

NETFLOW SPECIFIC SETTINGS

 If the target device sends incorrect time information that results in wrong monitoring data, please try to use **0** as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:

- **Off:** The standard flow will be used.
- **On:** Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.

CHANNEL CONFIGURATION

- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.
- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
 - ⚠ Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

💡 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

FILTERING

Include Filter Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

🔍 For detailed information, see section [Filter Rules](#)¹⁴¹⁴ below.

Exclude Filter First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

🔍 For detailed information, see section [Filter Rules](#)¹⁴¹⁴ below.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

- Primary Toplist** Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:
- **Top Talkers**
 - **Top Connections**
 - **Top Protocols**
 - **[Any custom toplists you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to NetFlow V5 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number

More

Paessler Website: Paessler NetFlow Testers

- <https://www.paessler.com/tools/netflowtester>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.88 NetFlow V5 (Custom) Sensor

The NetFlow V5 (Custom) sensor receives traffic data from a NetFlow V5 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor NetFlow V5 ★★★★☆
OK

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Top Talkers

Top Connections

Top Protocols

Take 'em all

Add Toplist

Total

3,015 kbit/s 0 19,298 kbit/s

FTP/P2P

0 kbit/s

Infrastructure

2,992 kbit/s

Mail

0 kbit/s

Other

0 kbit/s

Remote Control

0 kbit/s

Various

0 kbit/s

WWW

23 kbit/s

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
FTP/P2P	3002	0 KByte	0 kbit/s		
Infrastructure	3007	21,914 KByte	2,992 kbit/s	0 kbit/s	2,992 kbit/s
Mail	3003	0 KByte	0 kbit/s		
Other	0	0 KByte	0 kbit/s		
Remote Control	3005	0 KByte	0 kbit/s		
Total	-1	22,083 KByte	3,015 kbit/s	0 kbit/s	19,298 kbit/s
Various	3009	0 KByte	0 kbit/s	0 kbit/s	8,022 kbit/s
WWW	3001	169 KByte	23 kbit/s	0 kbit/s	8,284 kbit/s

NetFlow V5 Sensor

Sensor in Other Languages

Dutch: **NetFlow V5 (Klant specifiek)**, French: **NetFlow V5 (personnalisé)**, German: **NetFlow V5 (Benutzerdef.)**, Japanese: **NetFlow V5 (? ? ? ?)**, Portuguese: **NetFlow V5 (customizado)**, Russian: **NetFlow V5 (настраиваемый)**, Simplified Chinese: **NetFlow V5 (? ? ?)**, Spanish: **NetFlow V5 (Personalizado)**

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
 - This sensor [does not support more than 50 channels](#)¹⁴¹⁸ officially.
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	<p>Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value.</p> <p>i When configuring export, make sure you select the appropriate NetFlow version for this sensor.</p>
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on IP

Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you have configured in the NetFlow export options of your hardware router device.

 When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

Active Flow Timeout (Minutes)

Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown status**^[195]. Please enter an integer value.

We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

 If you set this value too low, flow information might be lost!

 For more details, see this Knowledge Base article: [What is the Active Flow Timeout in Flow sensors?](#)

 If the target device sends incorrect time information that results in wrong monitoring data, please try to use **0** as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:

- **Off:** The standard flow will be used.
- **On:** Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Channel Definition

Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined will be accounted to the default channel named **Other**.

NETFLOW SPECIFIC SETTINGS

 For detailed information, see section [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰.

 Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹⁴²⁷ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹⁴²⁷ below.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

PRIMARY TOPLIST

Primary Toplist	<p>Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:</p> <ul style="list-style-type: none">▪ Top Talkers▪ Top Connections▪ Top Protocols▪ [Any custom toplists you have added]
-----------------	--

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to NetFlow V5 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number

More

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

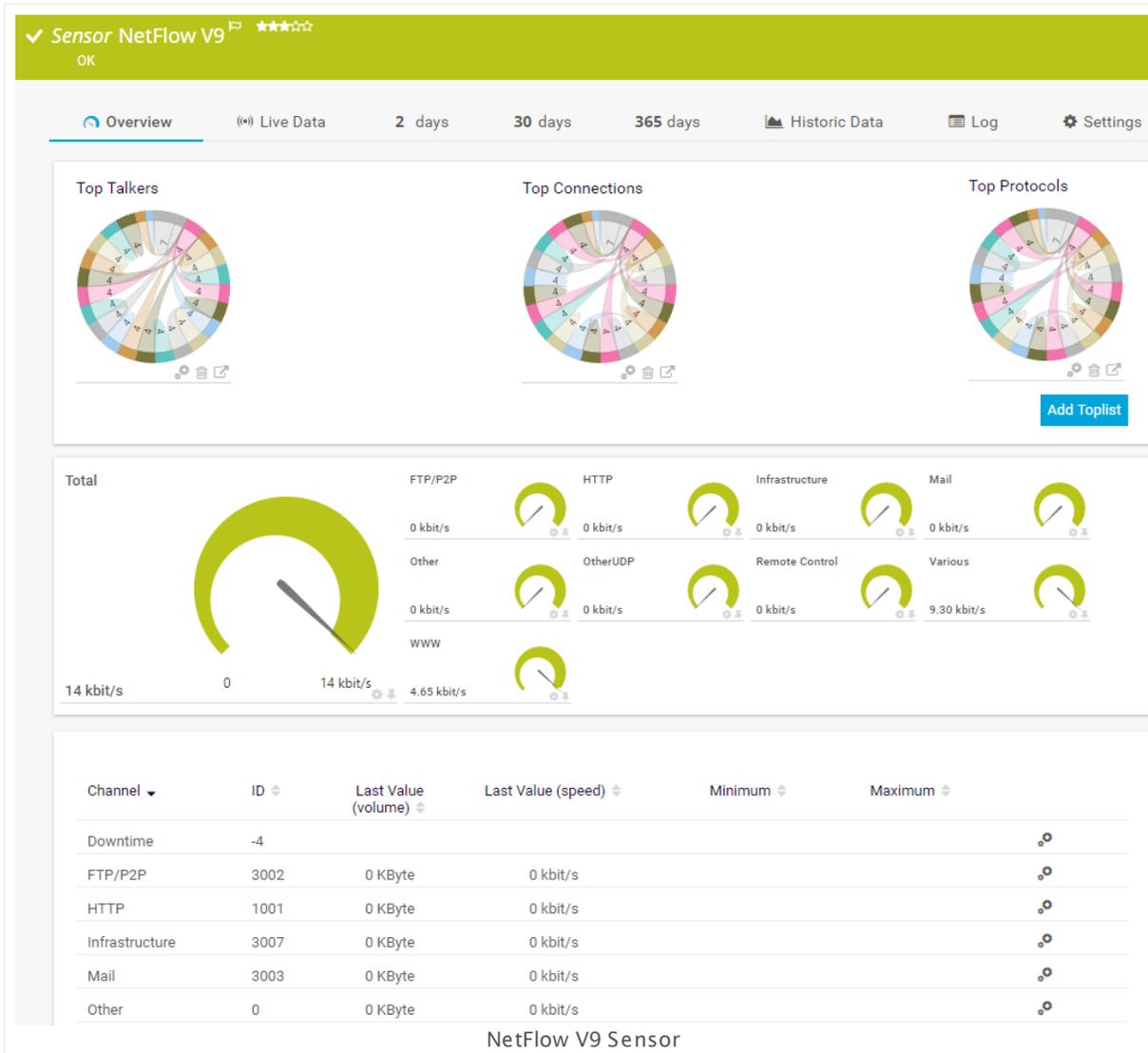
7.8.89 NetFlow V9 Sensor

The NetFlow V9 sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)
- Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
- For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#) [3514].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port

Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value.

 When configuring export, make sure you select the appropriate NetFlow version for this sensor.

Sender IP

Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

Receive NetFlow Packets on IP

Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address selected here must match the one you have configured in the NetFlow export options of your hardware router device.

 When configuring export, make sure you select the appropriate NetFlow version for this sensor.

Active Flow Timeout (Minutes)

Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown status**¹⁹⁵. Please enter an integer value.

We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

 If you set this value too low, flow information might be lost!

 For more details, see this Knowledge Base article: [What is the Active Flow Timeout in Flow sensors?](#)

 If the target device sends incorrect time information that results in wrong monitoring data, please try to use 0 as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:

NETFLOW SPECIFIC SETTINGS

- **Off:** The standard flow will be used.
- **On:** Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your exporter device. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection

Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.

CHANNEL CONFIGURATION

- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.
- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
 - ⚠ Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁴¹ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁴¹ below.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

PRIMARY TOPLIST

Primary Toplist	<p>Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:</p> <ul style="list-style-type: none">▪ Top Talkers▪ Top Connections▪ Top Protocols▪ [Any custom toplists you have added]
-----------------	--

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)  for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#) .

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats )
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats )
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats )
DestinationPort	Any number

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
89 NetFlow V9 Sensor

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to NetFlow V9 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).

FIELD	POSSIBLE FILTER VALUES
NextHop	IP address or DNS name (see Valid Data Formats ³⁶⁸⁸)
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

More

Paessler Website: Paessler NetFlow Testers

- <https://www.paessler.com/tools/netflowtester>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.90 NetFlow V9 (Custom) Sensor

The NetFlow V9 (Custom) sensor receives traffic data from a NetFlow V9 compatible device and shows the traffic by type. Please make sure the sensor matches the NetFlow version your device is exporting! In this custom sensor, you can define your own channel definitions to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
FTP/P2P	3002	0 KByte	0 kbit/s		
HTTP	1001	0 KByte	0 kbit/s		
Infrastructure	3007	0 KByte	0 kbit/s		
Mail	3003	0 KByte	0 kbit/s		
Other	0	0 KByte	0 kbit/s		

Sensor in Other Languages

Dutch: **NetFlow V9 (custom)**, French: **Net Flow V9 (personnalisé)**, German: **Net Flow V9 (Benutzerdef.)**, Japanese: **NetFlow V9 (? ? ? ?)**, Portuguese: **NetFlow V9 (customizado)**, Russian: **NetFlow V9 (настраиваемый)**, Simplified Chinese: **NetFlow V9 (? ? ?)**,

Spanish: **NetFlow V9 (Personalizado)**

Remarks

- You must enable NetFlow export of the respective version on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - Knowledge Base: [What is the Active Flow Timeout in Flow sensors?](#)
 - This sensor [does not support more than 50 channels](#)¹⁴⁴⁵ officially.
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on UDP Port	<p>Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the NetFlow export options of your hardware router device. Please enter an integer value.</p> <p>i When configuring export, make sure you select the appropriate NetFlow version for this sensor.</p>
Sender IP	Enter the IP address of the sending device you want to receive the NetFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

NETFLOW SPECIFIC SETTINGS

Receive NetFlow Packets on IP

Select the IP address(es) on which PRTG listens to NetFlow packets. The list of IP addresses you see here is specific to your setup. To select an IP address, add a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. The IP address you select here must match the one you have configured in the NetFlow export options of your hardware router device.

 When configuring export, please make sure you select the appropriate NetFlow version for this sensor.

Active Flow Timeout (Minutes)

Enter a time span in minutes after which new flow data must be received. If the timeout is reached and no new data was received during this time, the sensor switches to an **Unknown status**^[195]. Please enter an integer value.

We recommend that you set the timeout one minute longer than the respective timeout configured in your hardware router device. The maximum timeout is 60 minutes.

 If you set this value too low, flow information might be lost!

 For more details, see this Knowledge Base article: [What is the Active Flow Timeout in Flow sensors?](#)

 If the target device sends incorrect time information that results in wrong monitoring data, please try to use **0** as active flow timeout. This will ignore the start and stop information of a flow as provided by the device and account all data to the current point in time. It might result in spikes but all data will be captured.

Sampling Mode

Define if you want to use the sampling mode. This setting must match the setting in the flow exporter. Choose between:

- **Off:** The standard flow will be used.
- **On:** Switch into sampling mode and specify the sampling rate below.

Sampling Rate

This field is only visible when sampling mode is **On** above. Enter a number that matches the sampling rate in your device that exports the flows. If the number is different, monitoring results will be incorrect. Please enter an integer value.

Channel Definition

Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined will be accounted to the default channel named **Other**.

NETFLOW SPECIFIC SETTINGS

 For detailed information, see section [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰.

 Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.

Log Stream Data to Disk (for Debugging)

Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

FILTERING

Include Filter

Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁵⁴ below.

Exclude Filter

First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁵⁴ below.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

PRIMARY TOPLIST

Primary Toplist	<p>Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:</p> <ul style="list-style-type: none">▪ Top Talkers▪ Top Connections▪ Top Protocols▪ [Any custom toplists you have added]
-----------------	--

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to NetFlow V9 sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).

FIELD	POSSIBLE FILTER VALUES
NextHop	IP address or DNS name (see Valid Data Formats ³⁶⁸⁸)
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

More

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.91 Oracle SQL v2 Sensor

The Oracle SQL v2 sensor monitors a database on an Oracle server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows that were addressed by the query (including **select** statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Remarks

- [Requires](#) .NET 4.5 or later on the probe system.
- Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#) of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.

- PRTG Manual: [Monitoring Databases](#)^[3534] (includes an [example](#)^[3535] for channel value selection)
 - Knowledge Base: [How to setup the SQL v2 sensors in PRTG? Is there a guide?](#)
 - Knowledge Base: [How can I monitor strings from an SQL database and show a sensor status depending on it?](#)
 - Knowledge Base: [How can I monitor error tables in SQL databases?](#)
 - Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
 - Save the SQL script with the query into the `\Custom Sensors\sql\oracle` subfolder of your PRTG installation. See manual section [Data Storage](#)^[3731] for more information about how to find this path.
 - This sensor type supports Oracle database servers version 10.2 or higher
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Identifier	<p>Enter the Oracle System ID (SID) or the SERVICE_NAME of the database the sensor will connect to. Specify below which type of identifier you use. By default, the sensor uses the SID as connection string.</p> <p>The identifier is defined in the CONNECT_DATA part of the TNSNames.ora file on the Oracle instance. For example, a system ID can look like this: orcl</p>
Identification Method	<p>Define which type of identifier you use to connect to the database. This type depends on the configuration of your Oracle server. Choose between:</p> <ul style="list-style-type: none"> ▪ Use SID as identifier (default): Connect to the database instance using a system ID as connection string. Enter the SID above.

DATABASE SPECIFIC

- **Use SERVICE_NAME as identifier:** Connect to the database instance using a SERVICE_NAME as connection string. Enter the SERVICE_NAME above.

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific `\Custom Sensors\sql` subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

 For more information on how to find this path, see section [Data Storage](#). By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: **SELECT AVG (UnitPrice) FROM Products**. If you want to use transactions, separate the individual steps with semicolons ";".

 Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

 See also this Knowledge Base article: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

SQL Variables

You can use the following variables in your query file to have them replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: **@prt g**
- Oracle SQL: **:prt g**
- ADO SQL: **?** (question mark)

DATA

@prtg, **:prtg**, and **?** behave like common SQL variables, so consider the general rules for SQL variables. For example, you cannot use a variable for a table in the FROM statement of a query.

Example for variables usage: **SELECT * FROM Table WHERE @prtg**

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the variables **@prtg** (Microsoft SQL, MySQL, PostgreSQL), or **:prtg** (Oracle SQL), or **?** (ADO SQL) in the SQL query, considering the general rules for SQL variables. Choose between:

- **Don't use input parameter (default):** Execute the SQL query file without using variables.
- **Use input parameter:** Execute an SQL query file that contains a variable. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter will replace the variable **@prtg** or **:prtg** or **?** in the SQL query, considering the general rules for SQL variables.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, **%sensorid** or **%deviceid**. For details, see section [Custom Sensors](#)³⁶⁵⁴.

 Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default):** No transactions will be executed.
- **Use transaction and always rollback:** Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success:** Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

DATA

- **Just execute the query:** If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows:** Choose this option if you perform a **SELECT** statement and want to monitor how many rows of the data table this statement returns.
- **Process data table:** Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with **SELECT** statements as well.

Handle DBNull in Channel Values as

This setting is only visible if you select **Process data table** above. Define the sensor behavior if **DBNull** is returned by the query. Choose between:

- **Error:** The sensor will show a **Down** status if **DBNull** is reported.
- **Number 0:** The sensor will recognize the result **DBNull** as a valid value and interpret it as the number **0**.

Select Channel Value by

This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between:

- **Column number:** The channel value will be determined by using the value in row 0 of the column whose number you specify below.
- **Column name:** The channel value will be determined by using the value in row 0 of the column whose name you specify below.
- **Row number:** The channel value will be determined by using the value in column 0 of the row whose number you specify below.
- **Key value pair:** The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found.

The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below.

 See manual section [Monitoring Databases](#) ³⁵³⁴ for an [example](#) ³⁵³⁵ for channel value selection.

DATA

Sensor Channel #x This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for **Channel #1** without enabling it manually. For all other possible channels, choose between:

- **Disable:** This channel will not be added to the sensor.
- **Enable:** This channel will be added to the sensor. Define the settings as described above.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Column Number This setting is only visible if you select **Column number** above. Provide the number of the column that will be used to determine the channel value in row 0. Please enter an integer value.

Sensor Channel #x Column Name This setting is only visible if you select **Column number** above. Provide the name of the column that will be used to determine the channel value in row 0. Please enter a string.

Sensor Channel #x Row Number This setting is only visible if you select **Row number** above. Provide the number of the row that will be used to determine the channel value in column 0. Please enter an integer value.

Sensor Channel #x Key This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.

Sensor Channel #x Mode This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Absolute (recommended):** Shows the value as the sensor retrieves it from the data table.

DATA

- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from the data table. This mode is not compatible with the unit **Value Lookup**.

Sensor Channel #x
Unit

This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#).

 To use [lookups](#) with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

DATA

Sensor Channel #x Value Lookup	This settings is only visible if you select Value Lookup above. Select a lookup <small>3693</small> file that you want to use with this channel.
Use Data Table Value in Sensor Message	<p>This setting is only visible if you select Process data table above. Define if the sensor message will show a value from the data table. Choose between:</p> <ul style="list-style-type: none"> ▪ Disable: Do not use a custom sensor message. ▪ Enable: Define a custom sensor message with a defined value of the data table. Define the value selection below. <p>The method to determine a value for the sensor message is defined in setting Select Channel Value by above.</p>
Sensor Message Column Number	<p>This setting is only visible if you select Column number and Use Data Table Value in Sensor Message above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Column Name	<p>This setting is only visible if you select Column name and Use Data Table Value in Sensor Message above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Row Number	<p>This setting is only visible if you select Row number and Use Data Table Value in Sensor Message above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Key	<p>This setting is only visible if you select Key value pair and Use Data Table Value in Sensor Message above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message	<p>This setting is only visible if you select Use Data Table Value in Sensor Message above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.</p>

DATA

Example: **The message is {0}**

If Sensor Message Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³⁷⁷⁰ whenever the sensor value changes.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How to setup the SQL v2 sensors in PRTG? Is there a guide?

- <https://kb.paessler.com/en/topic/70618>

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Knowledge Base: How do I monitor the size of a Microsoft SQL server database?

- <https://kb.paessler.com/en/topic/18183>

Knowledge Base: How can I monitor error tables in SQL databases?

- <https://kb.paessler.com/en/topic/70774>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

PRTG Manual:

- [Monitoring Databases](#)³⁵³⁴

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.92 Oracle Tablespace Sensor

The Oracle Tablespace sensor monitors a tablespace on an Oracle server. It can show the following:

- Online status (online, system, recover, sysoff, offline, unknown)
- Status (available, invalid, unknown)
- Free disk space in bytes and percent
- Number of free blocks and in percent
- Current database size
- Database size on disk (managed tablespace)

Channel	ID	Last Value	Minimum	Maximum
Database Size	9	2.56 MByte	2.56 MByte	2.56 MByte
Database Size on Disk	10	100 MByte	100 MByte	100 MByte
Downtime	-4			
Free Blocks	7	1,441,464 #	1,441,464 #	1,441,464 #
Free Blocks %	8	>99 %	>99 %	>99 %
Free Space	5	11,261 MByte	11,261 MByte	11,261 MByte
Free Space %	6	>99 %	>99 %	>99 %
Online Status	3	ONLINE	ONLINE	ONLINE
Status	4	AVAILABLE	AVAILABLE	AVAILABLE

Oracle Tablespace Sensor

Sensor in Other Languages

Dutch: **Oracle Tablespace**, French: **Tablespace Oracle**, German: **Oracle Tablespace**, Japanese: **Oracle ? ? ? ? ? ? ? ?**, Portuguese: **Tablespace Oracle**, Russian: **Табличное пространство Oracle**, Simplified Chinese: **Oracle ? ? ?**, Spanish: **Espacio de tablas de Oracle**

Remarks

- This sensor type supports Oracle database servers version 10.2 or higher.
 - [Requires](#)¹⁴⁷⁵ .NET 4.5 or later on the probe system.
 - [Requires](#)¹⁴⁷⁵ sufficient privileges for the account that you use for the connection. We recommend that you use the **SYSTEM** account.
 - This sensor type does not support overprovisioning.
 - Knowledge Base: [Why is my Oracle Tablespace sensor showing negative values?](#)
 - Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#)⁴¹³ of the parent device, or in the settings of a group or probe above.
 - PRTG Manual: [Monitoring Databases](#)³⁵⁴
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶³.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)³⁷⁰. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Sufficient Account Privileges

Please use an account for the connection that has the privileges to see all (or specific) views. We recommend that you use the **SYSTEM** account if possible, otherwise grant your DBA the **SELECT_CATALOG_ROLE** to the account that you use. Without sufficient privileges you may see the error message **ORA-00942: table or view does not exist**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

In the appearing dialog box in the **Add Sensor** dialog, [enter an identifier](#)^[1477] to access the tablespace selection and click **OK**. Select the tablespaces in the Oracle database you want to monitor. PRTG creates one sensor for each tablespace you choose. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

TABLESPACE SPECIFIC

Tablespace	Select the tablespaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3262] , maps ^[3270] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ORACLE SPECIFIC

Identifier Enter the **Oracle System ID (SID)** or the **SERVICE_NAME** of the database the sensor will connect to. Specify below which type of identifier you use. By default, the sensor uses the SID as connection string.

The identifier is defined in the **CONNECT_DATA** part of the **TNSNames.ora** file on the Oracle instance. For example, a system ID can look like this: **orcl**

Identification Method Define which type of identifier that you use to connect to the database. This type depends on the configuration of your Oracle server. Choose between:

- **Use SID as identifier (default):** Connect to the database instance using a system ID as connection string. Enter the SID above.
- **Use SERVICE_NAME as identifier:** Connect to the database instance using a SERVICE_NAME as connection string. Enter the SERVICE_NAME above.

Sensor Name Prefix Define if you want to use the **SERVICE_NAME** as prefix for the sensor name. If you have multiple databases on your Oracle server, this will help you to distinguish the monitored tablespaces. Choose between:

- **Do not use a prefix for the sensor name:** The sensor name will only show the name of the monitored tablespace.
- **Use SERVICE_NAME as prefix for the sensor name:** PRTG will add the **SERVICE_NAME** to the beginning of the sensor name.

ORACLE SPECIFIC

TABLESPACE SPECIFIC

Tablespace Shows the tablespace that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Knowledge Base: Why is my Oracle Tablespace sensor showing negative values?

- <https://kb.paessler.com/en/topic/79066>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

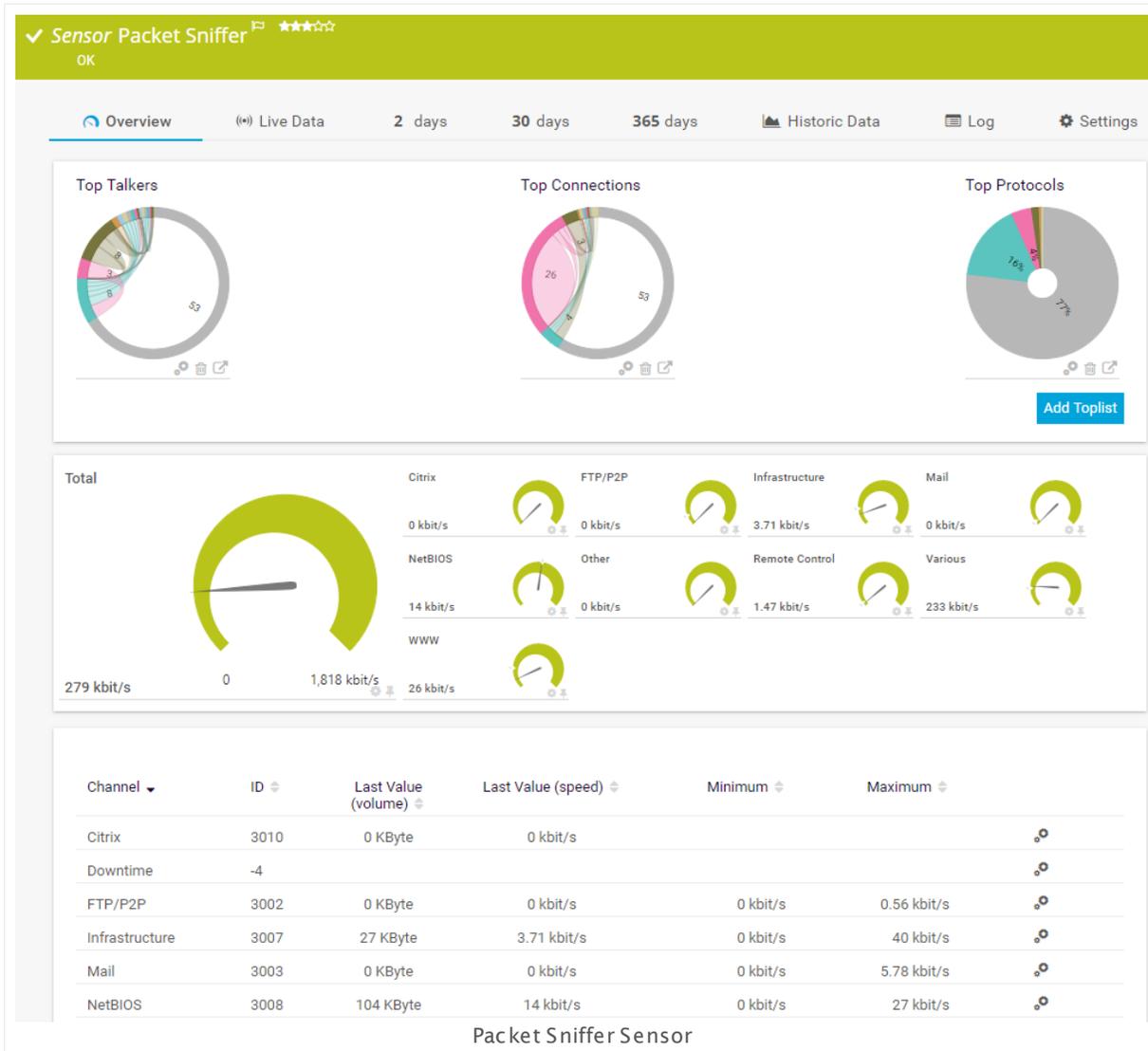
7.8.93 Packet Sniffer Sensor

The Packet Sniffer sensor monitors the headers of data packets that pass a local network card using a built-in packet sniffer. You can choose from predefined channels. The sensor analyzes only header traffic.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Packet Sniffer**, French: **Packet sniffing**, German: **Packet Sniffer**, Japanese: ? ? ? ? ? ? ? ? , Portuguese: **Sniffer de pacotes**, Russian: **Анализатор пакетов**, Simplified Chinese: ? ? ? ? ? ? , Spanish: **Esniifer de paquetes**

Remarks

- By default, this sensor works only on a probe device.
- Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)
- For a general introduction to the technology behind packet sniffing, see manual section [Monitoring Bandwidth via Packet Sniffing](#) ³⁶¹².

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

i By default, you can only monitor traffic passing the PRTG probe system where the **Probe Device** with the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNIFFER SPECIFIC

Include Filter Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁹⁴ below.

Exclude Filter First, the filters you define in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹⁴⁹⁴ below.

Network Adapters Define the network adapters that this sensor monitors. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name. You can also select and deselect all items by using the check box in the table head.

Log Stream Data to Disk (for Debugging) Define if the probe will write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. We recommend this for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

SNIFFER SPECIFIC

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.
- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.
- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
 -  Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

CHANNEL CONFIGURATION

 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**

PRIMARY TOPLIST

- **Top Protocols**
- **[Any custom toplists you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. |

SCANNING INTERVAL

- **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)  for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#) .

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats )
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats )
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats )

FIELD	POSSIBLE FILTER VALUES
DestinationPort	Any number
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to Packet Sniffer sensors only.

FIELD	POSSIBLE FILTER VALUES
MAC	Physical address (see Examples )
SourceMAC	Physical address
DestinationMAC	Physical address
EtherType	IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, any number
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to TOS used with IPv4
FlowLabel	IPv6 Flow Label

More

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.94 Packet Sniffer (Custom) Sensor

The Packet Sniffer (Custom) sensor monitors the headers of data packets that pass a local network card using built-in packet sniffer. You can define your own channels. There are no predefined channels for this sensor type. This sensor analyzes only header traffic.

- This sensor can show traffic by type individually to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor Packet Sniffer ☆☆☆☆
OK

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Top Talkers

Top Connections

Top Protocols

[Add Toplist](#)

Total

279 kbit/s

Citrix

0 kbit/s

NetBIOS

14 kbit/s

WWW

26 kbit/s

FTP/P2P

0 kbit/s

Other

0 kbit/s

Infrastructure

3.71 kbit/s

Remote Control

1.47 kbit/s

Mail

0 kbit/s

Various

233 kbit/s

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Citrix	3010	0 KByte	0 kbit/s		
Downtime	-4				
FTP/P2P	3002	0 KByte	0 kbit/s	0 kbit/s	0.56 kbit/s
Infrastructure	3007	27 KByte	3.71 kbit/s	0 kbit/s	40 kbit/s
Mail	3003	0 KByte	0 kbit/s	0 kbit/s	5.78 kbit/s
NetBIOS	3008	104 KByte	14 kbit/s	0 kbit/s	27 kbit/s

Packet Sniffer Sensor

Sensor in Other Languages

Dutch: **Packet Sniffer (Klant specifiek)**, French: **Packet Sniffer (personnalisé)**, German: **Packet Sniffer (Benutzerdef.)**, Japanese: **???????? (????)**, Portuguese: **Sniffer de pacotes (Customizado)**, Russian: **Анализатор пакетов (нестандартный)**, Simplified Chinese: **?????? (????)**, Spanish: **Esnifer de paquetes (personalizado)**

Remarks

- By default, this sensor works only on a probe device.
- This sensor [does not support more than 50 channels](#)^[1498] officially.
- For a general introduction to the technology behind packet sniffing, see manual section [Monitoring Bandwidth via Packet Sniffing](#)^[3512].
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

i By default, you can only monitor traffic passing the PRTG probe system where the **Probe Device** with the sensor is set up (either a local or remote probe). To monitor other traffic in your network, you can configure a monitoring port (if available) that the switch sends a copy of all traffic to. You can then physically connect this port to a network card of the computer the PRTG probe (either local or remote probe) is running on. This way, PRTG can analyze the complete traffic that passes through the switch. This feature of your hardware may be called Switched Port Analyzer (SPAN), port mirroring, or port monitoring.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

! PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNIFFER SPECIFIC

Include Filter	<p>Define if you want to filter any traffic. If you leave this field empty, the sensor includes all traffic. To include specific traffic only, define filters using a special syntax.</p> <p> For detailed information, see section Filter Rules below.</p>
Exclude Filter	<p>First, the filters you define in the Include Filter field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.</p> <p> For detailed information, see section Filter Rules below.</p>

SNIFFER SPECIFIC

Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined is accounted to the default channel named Other.</p> <p> For detailed information, see section Channel Defintions for xFlow and Packet Sniffer Sensors³⁶⁹⁰.</p> <p> Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze. We recommend that you do not use more than 20 channels in graphs and tables, and not more than 100 channels in total. For performance reasons, it is better to add several sensors with less channels each.</p>
Network Adapters	<p>Define the network adapters that this sensor monitors. You see a list of names with all adapters available on the probe system. To select an adapter, set a check mark symbol in front of the respective name. You can also select and deselect all items by using the check box in the table head.</p>
Log Stream Data to Disk (for Debugging)	<p>Define if the probe will write a logfile of the stream and packet data to the data folder (see Data Storage³⁷³⁴). Choose between:</p> <ul style="list-style-type: none"> ▪ None (recommended): Do not write additional logfiles. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write logfiles for all data received. <p> Use with caution! Enabling this option might create huge data files. Please use for a short time and for debugging purposes only.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
-----------------	---

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

PRIMARY TOPLIST

Primary Toplist	<p>Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:</p> <ul style="list-style-type: none"> ▪ Top Talkers ▪ Top Connections ▪ Top Protocols ▪ [Any custom toplists you have added]
-----------------	---

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to Packet Sniffer sensors only.

FIELD	POSSIBLE FILTER VALUES
MAC	Physical address (see Examples )
SourceMAC	Physical address
DestinationMAC	Physical address
EtherType	IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, any number
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to TOS used with IPv4
FlowLabel	IPv6 Flow Label

More

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)  section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

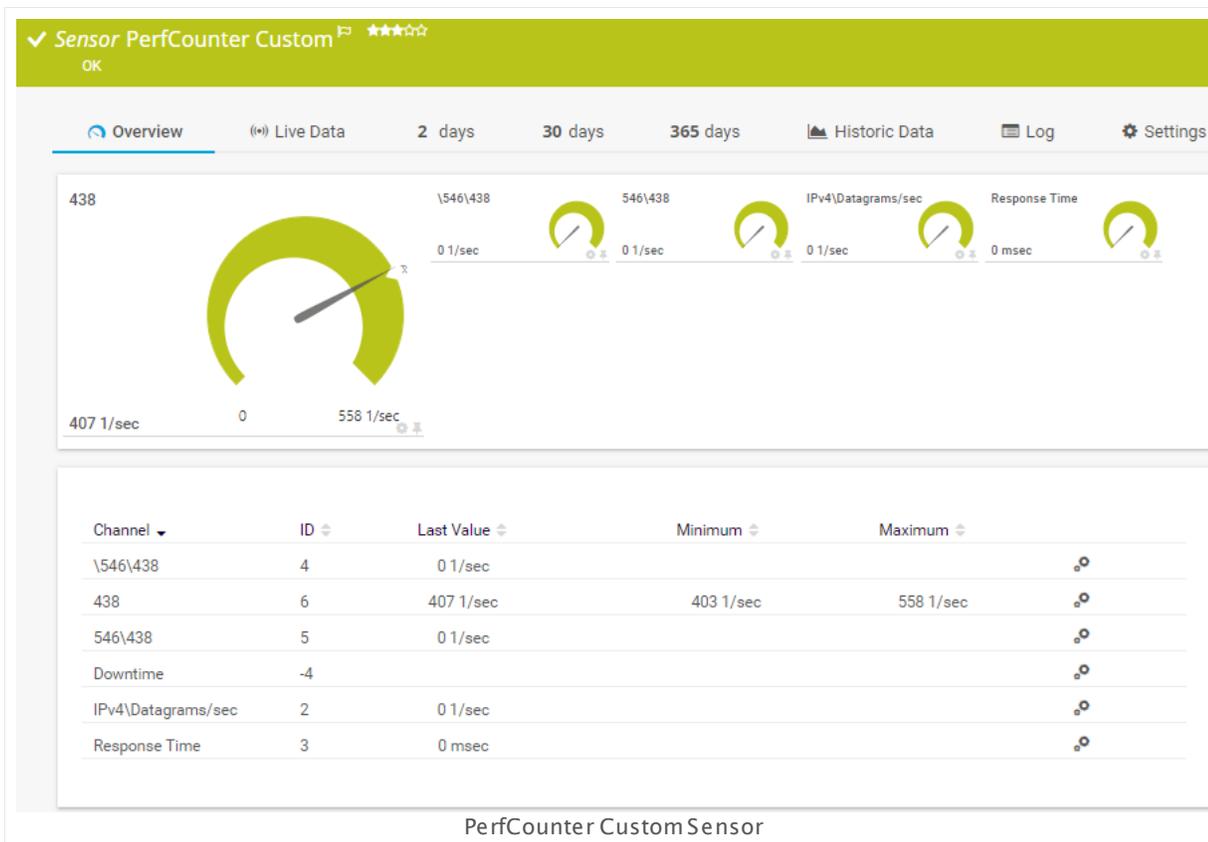
7.8.95 PerfCounter Custom Sensor

The PerfCounter Custom sensor monitors a configured set of Windows Performance Counters. You can define your own channels. There are no predefined channels available for this sensor type.

- This sensor can show Windows Performance Counters individually to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

 To find available performance counters and their names on the target system, see this Knowledge Base article: [How can I find out the names of available Performance Counters?](#)



Sensor in Other Languages

Dutch: **Prestatie Meters Klant specifiek**, French: **PerfCounter personnalisé**, German: **Leistungsindikator (benutzerdef.)**, Japanese: ??????????????????, Portuguese: **PerfCounter (Customizado)**, Russian: **Специальные настройки PerfCounter**, Simplified Chinese: ??????????, Spanish: **PerfCounter Personalizado**

Remarks

- [Requires](#)  Windows credentials in the parent device settings.

- [Requires](#)^[1510] the Windows Remote Registry service to be running on the target computer.
 - [Requires](#)^[1510] Windows Server 2008 R2 or later on the probe system.
 - Knowledge Base: [How can I find out the names of available Performance Counters?](#)
 - Knowledge Base: [My Performance Counter sensor does not work. What can I do?](#)
 - You cannot add different performance counters with the same name to one sensor.
 - If a performance counter contains angle brackets (< or >), please do not edit the channel settings because this might cause an error.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

-  Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.
-  If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.
-  The user account has to be a member of the **Performance Monitor Users** user group on the target system.

Requirement: Remote Registry Service

-  In order for this sensor to work with Windows Performance Counters, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Version

-  In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 R2 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[3705].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

PERFORMANCE COUNTER SETTINGS

List of Counters

Enter a list of performance counters that will be queried. Define one counter per row. PRTG will create one channel for each counter. Use the following syntax: the name of the counter, followed by two colons (::) and the unit.

Example: `\Processor(_Total)\% Processor Time::%`

 It is not possible to monitor different performance counters with the same name in one sensor. The sensor uses the counter as channel name, so this would create duplicate channels, which PRTG does not support. If you want to monitor different performance counters with the same name, please add one sensor for each counter. You can also create a [custom sensor](#)³¹⁵⁵. For example, you can write a PowerShell query that connects to the target device, retrieves the desired counters with the `Get-Counter` cmdlet, and reports them back to PRTG as individual channels.

 If your custom performance counter includes an angle bracket (< or >), please do not edit the [Sensor Channels Settings](#)³¹⁶⁰ (for example, limits) after creating the sensor! This might lead to a malfunctioning sensor.

Mode

Define the mode for the return value of the performance counter. This setting determines if the returning value will be displayed as absolute value or if the difference between the last and the current value will be used. Choose between:

- **Absolute (recommended):** The returning value will be displayed as absolute value.
 - **Difference:** The difference between last and current value will be displayed.
-  Make sure that all counters that you monitor are capable of this mode if you select it.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PERFORMANCE COUNTER SETTINGS

List of Counters	Shows the performance counters that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Mode	Shows the mode in which the sensor displays the returning values. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I find out the names of available Performance Counters?

- <https://kb.paessler.com/en/topic/50673>

Knowledge Base: Remote Monitoring of Specific Performance Counters

- <https://kb.paessler.com/en/topic/59804>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.96 PerfCounter IIS Application Pool Sensor

The PerfCounter IIS Application Pool sensor monitors a Microsoft Internet Information Services (IIS) application pool using Windows Performance Counters.

It can show the following:

- Overall status of the application pool:
 - Running ([sensor status](#) ¹⁹⁵ **Up**)
 - Initialized or Shutdown Pending (**Warning**)
 - Unavailable, Uninitialized, Stopping, Stopped, or Delete Pending (**Down**)
- Number of worker processes
- Number of failures in worker processes per second
- Number of ping failures per second
- Number of shutdown failures per second
- Number of startup failures per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Application Pool St...	0	Running		Running	Running
Downtime	-4				
Worker Process Fai...	2	0 #	0 #/s	0 #/s	0 #/s
Worker Process Pin...	3	0 #	0 #/s	0 #/s	0 #/s
Worker Process Sh...	4	0 #	0 #/s	0 #/s	0 #/s
Worker Process Sta...	5	0 #	0 #/s	0 #/s	0 #/s
Worker Processes	1	0 #		0 #	0 #

PerfCounter IIS Application Pool Sensor

Sensor in Other Languages

Dutch: **PerfCounter IIS Application Pool**, French: **Pool d'application IIS PerfCounter**, German: **Leistungsindikator IIS-Anwendungspool**, Japanese: **?? ? ? ? ? ? ? ? ? IIS ? ? ? ? ? ? ? ? ? ?**, Portuguese: **Pool de aplicativos IIS via PerfCounter**, Russian: **Пл приложений IIS (PerfCounter)**, Simplified Chinese: **?? ? ? ? IIS ? ? ? ? ?**, Spanish: **Grupo de aplicaciones PerfCounter IIS**

Remarks

- [Requires](#)¹⁵²⁰ Microsoft IIS version 7.5 or later on the target system.
- [Requires](#)¹⁵²⁰ Windows credentials in the parent device settings.
- [Requires](#)¹⁵²⁰ the Windows Remote Registry service to be running on the target computer.
- [Requires](#)¹⁵²¹ Windows Server 2008 R2 or later on the probe system.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Microsoft IIS Version 7.5

 To monitor Microsoft Internet Information Services (IIS) application pools, this sensor needs IIS version 7.5 or later to be installed on the target system.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)⁴⁰⁷ **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

 The user account has to be a member of the **Performance Monitor Users** user group on the target system.

Requirement: Remote Registry Service

 In order for this sensor to work with Windows Performance Counters, please make sure the **RemoteRegistry** "Remote Registry" Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 R2 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[370].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Microsoft Internet Information Services (IIS) application pools that you want to monitor. PRTG creates one sensor for each pool you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IIS APPLICATION POOL SPECIFIC

Application Pool	Select the application pools you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IIS APPLICATION POOL SPECIFIC

Application Pool	Shows the name of the application pool that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------------------	--

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

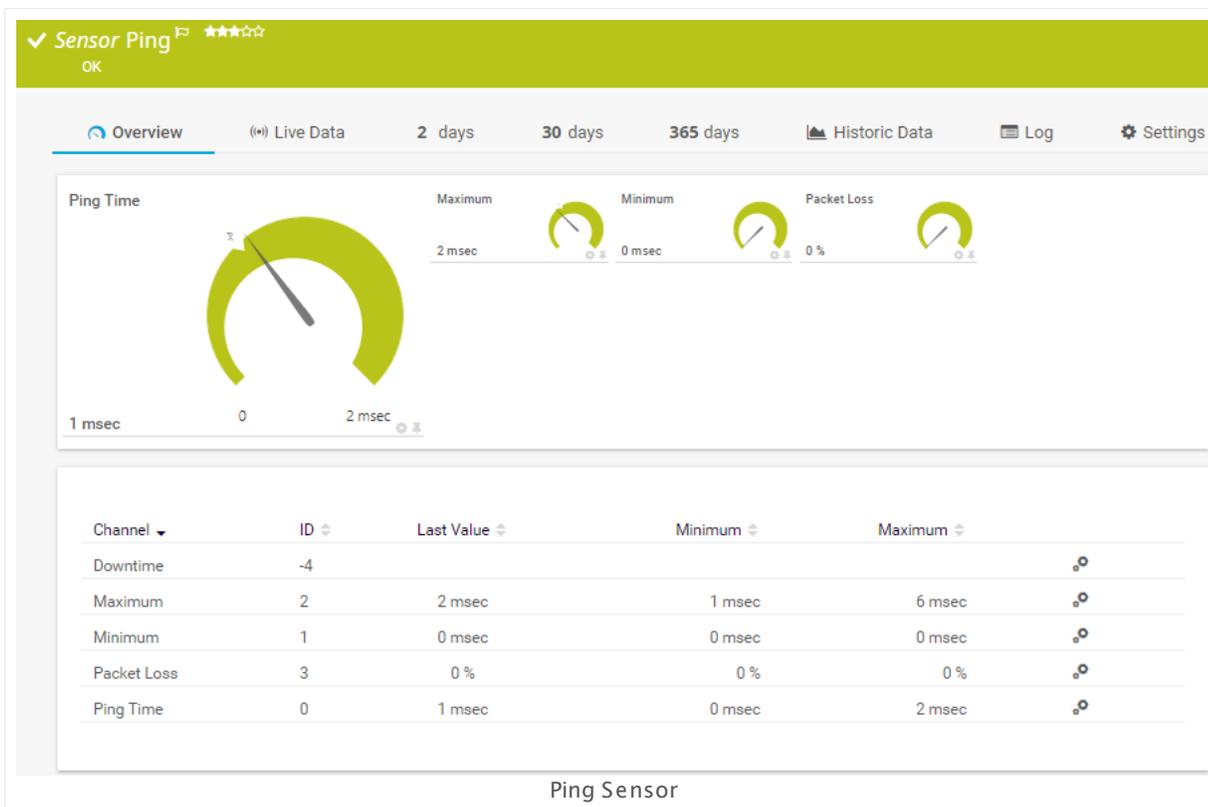
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.97 Ping Sensor

The Ping sensor sends an Internet Control Message Protocol (ICMP) echo request ("Ping") from the computer running the probe to the device it is created on to monitor the availability of a device. Default is 5 Pings per scanning interval.

It can show the following:

- Ping time
- Minimum Ping time when using more than one Ping per interval
- Maximum Ping time when using more than one Ping per interval
- Packet loss in percent when using more than one Ping per interval



Remarks

- Knowledge Base: [How to create/customize statistical PING sensor?](#)
- Knowledge Base: [Can I create an inverse Ping sensor?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PING SETTINGS

Timeout (Sec.)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the sensor will cancel the request and show an error message. The maximum timeout value is 300 seconds (5 minutes).
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can choose any value between 1 and 10000 . We recommend that you use the default value.
Ping Method	Define the kind of Ping check that the sensor performs. Choose between: <ul style="list-style-type: none">▪ Send one single Ping: With each scanning interval, send a single Ping only. A sensor in this setting will show the Ping time only. This setting is good for simple availability monitoring.▪ Send multiple Ping request: With each scanning interval, send multiple Pings in a row. A sensor in this setting will also show minimum and maximum Ping time as well as packet loss (in percent). This setting is good if you want to create reports about average Ping times out of a series of ping requests. This is the default setting.<ul style="list-style-type: none">❗ When using multiple requests, all of them have to be lost to show a Down status^[195]. For example, if there is only one Ping request answered in a series of five, the sensor will still show a green Up status.
Ping Count	This field is only visible if you enable Send multiple Ping request above. Enter the number of Pings that the sensor sends in a row for one interval. Please enter an integer value. The default value is 5 .
Ping Delay (in ms)	This field is only visible if you enable Send multiple Ping request above. Enter the time in milliseconds the sensor waits between two Ping requests. Please enter an integer value. The default value is 5 . <ul style="list-style-type: none">❗ Increase the value if the target device drops Ping packets due to denial-of-service (DOS) suspicion.
Auto Acknowledge	You can define that a Down status of this sensor will be acknowledged ^[220] automatically. <ul style="list-style-type: none">▪ Show "Down" status on error (default): Do not automatically acknowledge an alarm if this sensor changes to a Down status.▪ Show "Down (Acknowledged)" status on error: Automatically acknowledge an alarm. If this sensor changes to a Down status, it will automatically show Down (Acknowledged) instead.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How to create/customize statistical PING sensor?

- <https://kb.paessler.com/en/topic/1873>

Knowledge Base: Can I create an inverse Ping sensor?

- <https://kb.paessler.com/en/topic/10203>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.98 Ping Jitter Sensor

The Ping Jitter sensor sends a series of Internet Control Message Protocol (ICMP) echo requests ("Pings") to the given URI to determine the statistical jitter.

This sensor shows the following:

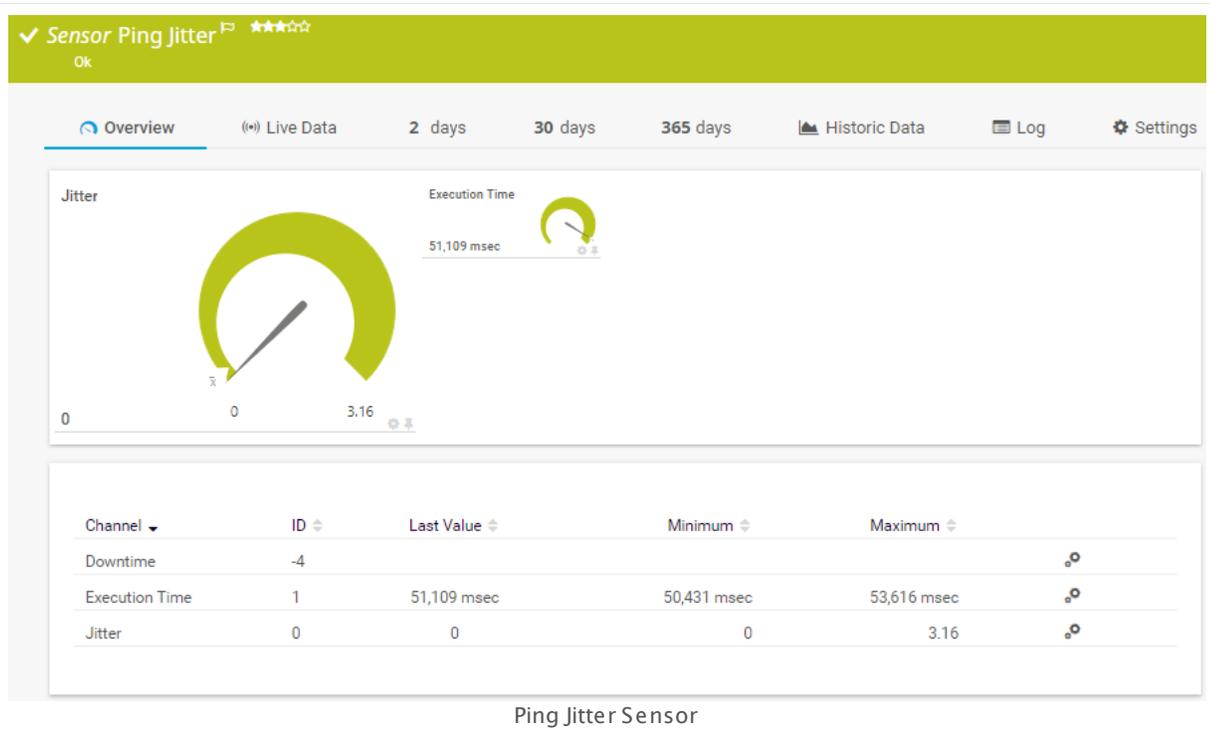
- Statistical jitter value
- Execution time

The Real Time Jitter value is updated every time a packet is received using the formula described in RFC 1889:

```
Jitter = Jitter + ( abs( ElapsedTime - OldElapsedTime ) - Jitter ) / 16
```

The Statistical Jitter value is calculated on the first x packets received using the statistical variance formula:

```
Jitter Statistical = SquareRootOf( SumOf( ( ElapsedTime[i] - Average ) ^ 2 ) / ( ReceivedPacketCount - 1 )
```



Sensor in Other Languages

Dutch: **Ping Jitter**, French: **Gigue du ping**, German: **Ping Jitter**, Japanese: **PI ng JI tter ? ?**, Portuguese: **Ping Jitter**, Russian: **Флуктуация Ping**, Simplified Chinese: **Ping ? ?**, Spanish: **Jitter de Ping**

Remarks

- [Requires](#) ¹⁶³⁹ .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ¹⁸¹ , as well as in alarms ²¹⁹ , logs ²²⁸ , notifications ³²¹⁶ , reports ³²⁵² , maps ³²⁷⁶ , libraries ³²³⁵ , and tickets ²³⁰ .
Parent Tags	Shows Tags ¹³⁹ that this sensor inherits ¹⁴⁰ from its parent device, group, and probe ¹³³ . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

- Ping Count** Define the number of Internet Control Message Protocol (ICMP) pings that this sensor sends. Please enter an integer value.

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

DEBUG OPTIONS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
98 Ping Jitter Sensor

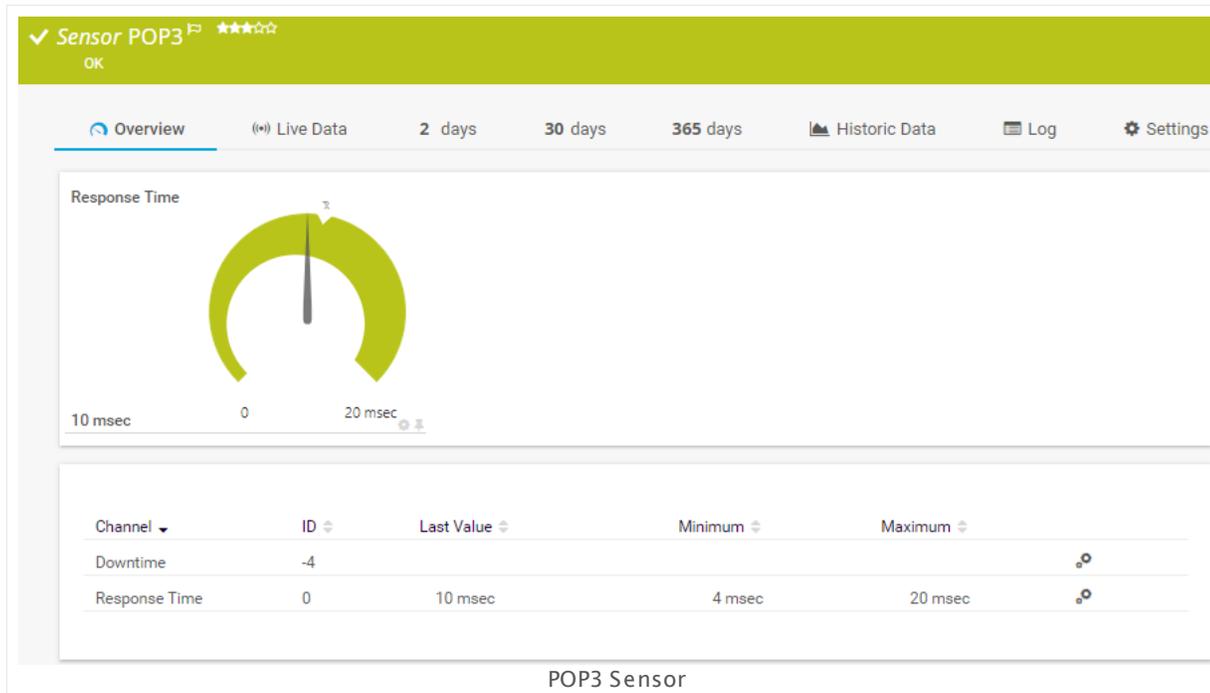
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.99 POP3 Sensor

The POP3 sensor monitors an email server using Post Office Protocol version 3 (POP3).

- It shows the response time of the server.



Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

POP3 SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	<p>Specify the port that the sensor uses for the POP3 connection. This is usually port 110 for non-secure connections and usually port 995 for SSL connections. The actual setting depends on the server you are connecting to. Please enter an integer value. We recommend that you use the default value.</p> <p> If you do not get a connection, please try another port number.</p>

TRANSPORT-LEVEL SECURITY

Sensor Specific

Define the security level for the sensor connection. Choose between:

- **Use Transport-Level Security if available using StartTLS (default):** Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.
 - **Use Transport-Level Security if available:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
 - **Enforce Transport-Level Security using StartTLS:** Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down status**^[195].
 - **Enforce Transport-Level Security:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down status**^[195].
- i** If the sensor connects to a server via **StartTLS**, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.
- i** If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

POP3 AUTHENTICATION

Type	<p>Select the kind of authentication for the POP3 connection. Choose between:</p> <ul style="list-style-type: none"> ▪ Without login: Monitor the connection to the POP3 server only. ▪ Username and password: Log in to the POP3 server with username and password (simple login, non-secure). ▪ 128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you connect to.
Username	<p>This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.</p>
Password	<p>This field is only visible if you select an option with login above. Enter a password for POP3 authentication. Please enter a string.</p>
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> For more information on how to find the folder used for storage, see section Data Storage. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
-----------------	---

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[336] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

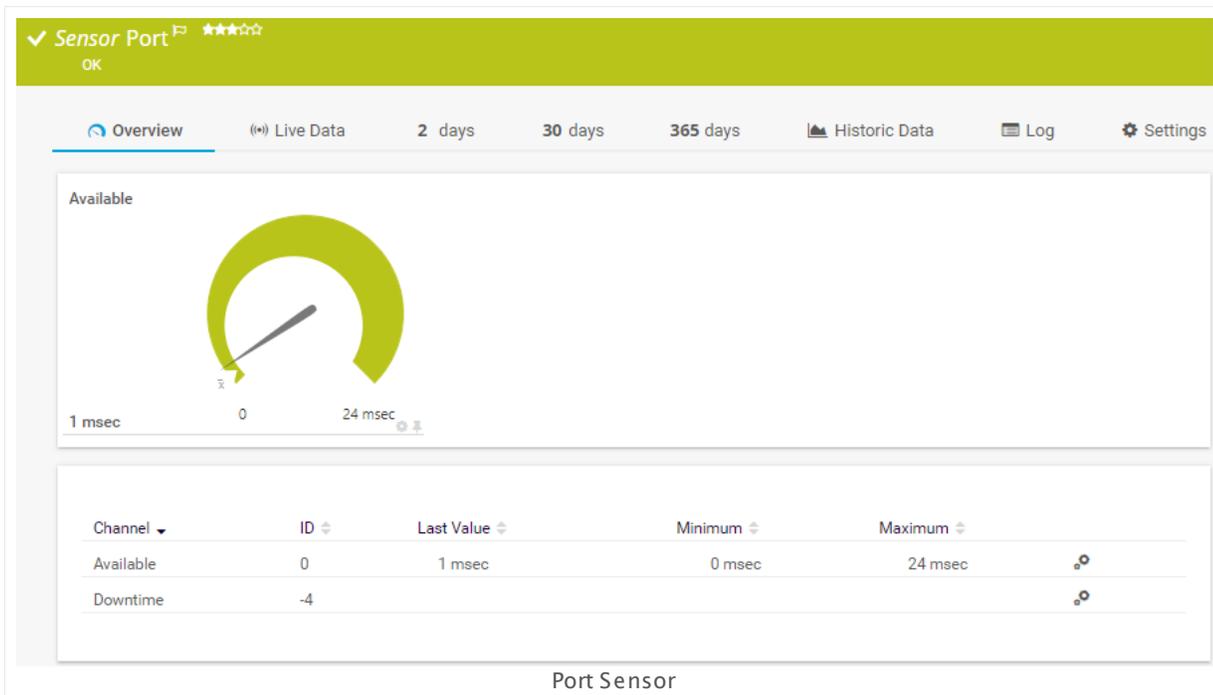
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.100 Port Sensor

The Port sensor monitors a network service by connecting to its port. It tries to connect to the specified TCP/IP port number of a device and waits for the request to be accepted. Depending on your settings, it can alert you either when the monitored port is open, or when it is closed.

- The sensor shows the time until a request to a port is accepted.



Sensor in Other Languages

Dutch: **Poort**, French: **Port**, German: **Port**, Japanese: ? ? ? , Portuguese: **Porta**, Russian: **Порт**, Simplified Chinese: ? ? , Spanish: **Puerto**

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PORT SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value.

TRANSPORT-LEVEL SECURITY

- Security** Define the security level for the sensor connection. Choose between:
- **Use Transport-Level Security (default):** Establish the connection with the strongest TLS method that the target device provides.
 - **Do not use Transport-Level Security:** Establish the connection without encryption.

ADVANCED SENSOR SETTINGS

- Goal** Define how the sensor will report on the port defined above. Choose between:
- **Open:** The sensor shows a green **Up status** ¹⁹⁵ if the port is open, and a red **Down** status if the port is closed.
 - **Closed:** The sensor shows a green **Up status** ¹⁹⁵ if the port is closed, and a red **Down** status if the port is open.
- Command** Define whether the sensor will send a command after opening the port. Choose between:
- **Don't send command:** Only check if a connection to the port is possible.
 - **Send command:** Open a Telnet session to the respective port and send the command.
 - ❗ You cannot use this option if the target machine is a web server.
- Command** This field is only visible if you enable **Send command** above. Enter a command that the sensor sends in a Telnet session to the respective port. You cannot use line breaks, only a simple Telnet command in a single line. Please enter a string.
- Response** Define if the sensor will process the received response further. Choose between:
- **Ignore response:** Do not check the response.
 - **Check response code (integer):** Check if the response matches a defined response code. Define below.

ADVANCED SENSOR SETTINGS

- **Check response text:** Check if the response matches a defined response text. Define below.

Allowed Code

This field is only visible if you enable **Check response code (integer)** above. Enter a code that the target device must return. If it does not match, the sensor will show a **Down status**^[195]. Please enter an integer value.

Check For Existing
Keywords (positive)

This setting is only visible if you activated **Check response text** above. Check if a certain keyword is part of the received value. If there is no match, the sensor will show a **Down status**^[195].

- **Disable:** Do not check for positive keywords.
- **Enable keyword check (positive):** Check if a certain keyword exists in the received value. Define below.

Response Must Include

This setting is only visible if you activate keyword check above. Enter a search string that the returned value must contain.

For Keyword Search
Use

Define the method that you want to use for the search string. Choose between:

- **Plain Text:** Search for a simple string.
- **Regular Expression:** Search using a regular expression. For more details, see [Regular Expressions](#)^[3704] section.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

Check For Existing
Keywords (negative)

This setting is only visible if you activated text processing above. Check if a certain keyword is **not** part of the received value. If there **is** a match, the sensor will show a **Down status**^[195].

- **Disable:** Do not check for negative keywords.
- **Enable keyword check (negative):** Check if a certain keyword does not exist in the received value. Define below.

Text Must Not Include

This setting is only visible if you activate keyword check above. Enter a search string that the returned value must **not** contain.

For Keyword Search
Use

Define the method you want to use for the search string. Choose between:

- **Plain Text:** Search for a simple string.

- **Regular Expression:** Search using a regular expression. For more details, see [Regular Expressions](#)³⁷⁰⁴ section.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)³⁷⁰⁴.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

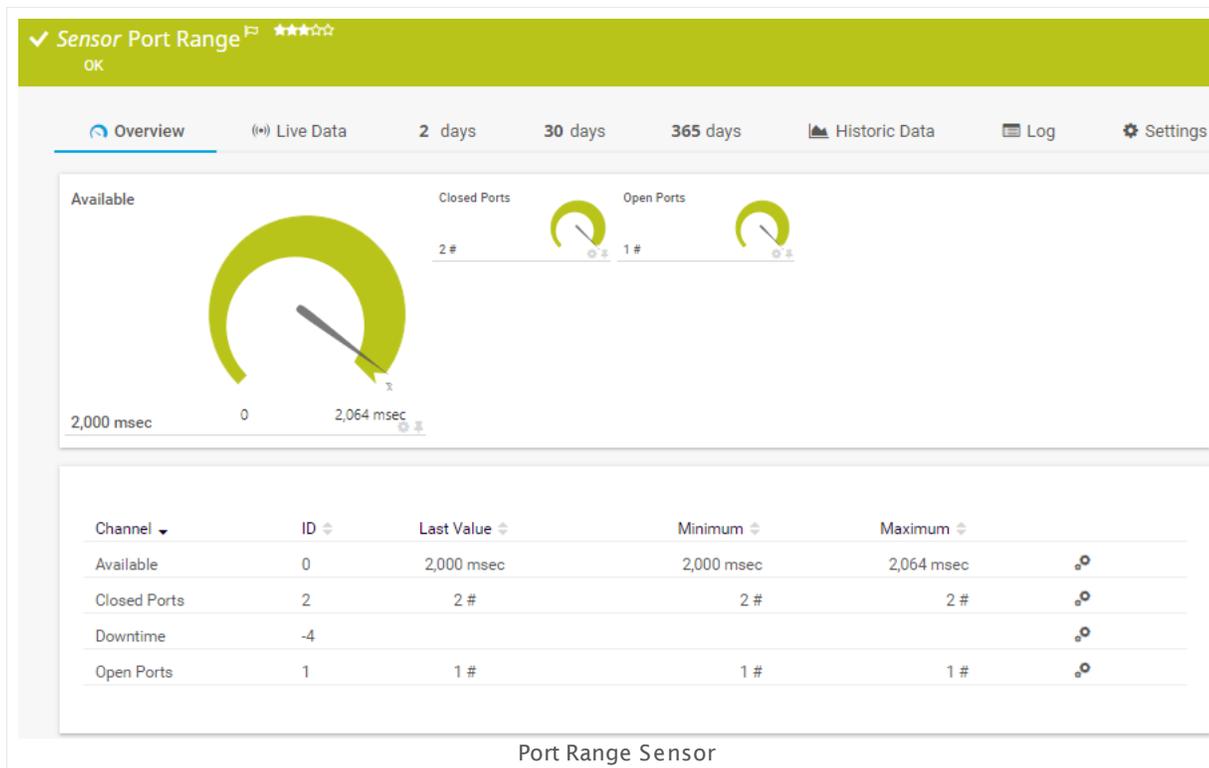
7.8.101 Port Range Sensor

The Port Range sensor monitors a network service by connecting to various TCP/IP ports. It tries to connect to the specified TCP/IP port numbers of a device in succession and waits for each request to be accepted.

It shows the following:

- Number of closed ports
- Number of open ports
- Time until requests are accepted

Optionally, you can set limits in the [sensor channel settings](#). This way you can get alerts about open and closed ports.



Sensor in Other Languages

Dutch: **Poort bereik**, French: **Plage de port**, German: **Port bereich**, Japanese: ? ? ? ? ? ,
 Portuguese: **Intervalo de portas**, Russian: **диапазон портов**, Simplified Chinese: ? ? ? ? ,
 Spanish: **Rango de puerto**

Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PORT RANGE SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port-by-Port-Delay (ms)	Specify in milliseconds how long the sensor will wait to go to the next port while running through all given ports.
Port Range Selection Method	Define whether you want to monitor all ports within a range or if you want to monitor several individual ports. Choose between: <ul style="list-style-type: none"> ▪ Port range with start/end: Monitor ports within a range. ▪ List of ports: Monitor several individual ports.
Range Start	This field is only visible if you enable Port range with start/end above. Enter the port number where the scan starts. Please enter an integer value.
Range End	This field is only visible if you enable Port range with start/end above. Enter the port number where the scan ends. Please enter an integer value.
Port List	This field is only visible if you enable List of ports above. Enter the numbers of the ports the sensor will try to connect to. Enter one or more individual integer values, each port in one line.
If Value Changes	Define what the sensor will do if the number of closed ports or open ports changes. Choose between: <ul style="list-style-type: none"> ▪ Ignore changes: No action is taken on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>3170</small> whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend
-----------------	--

SENSOR DISPLAY

on what channels are available for this sensor.

- ❗ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ❗ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

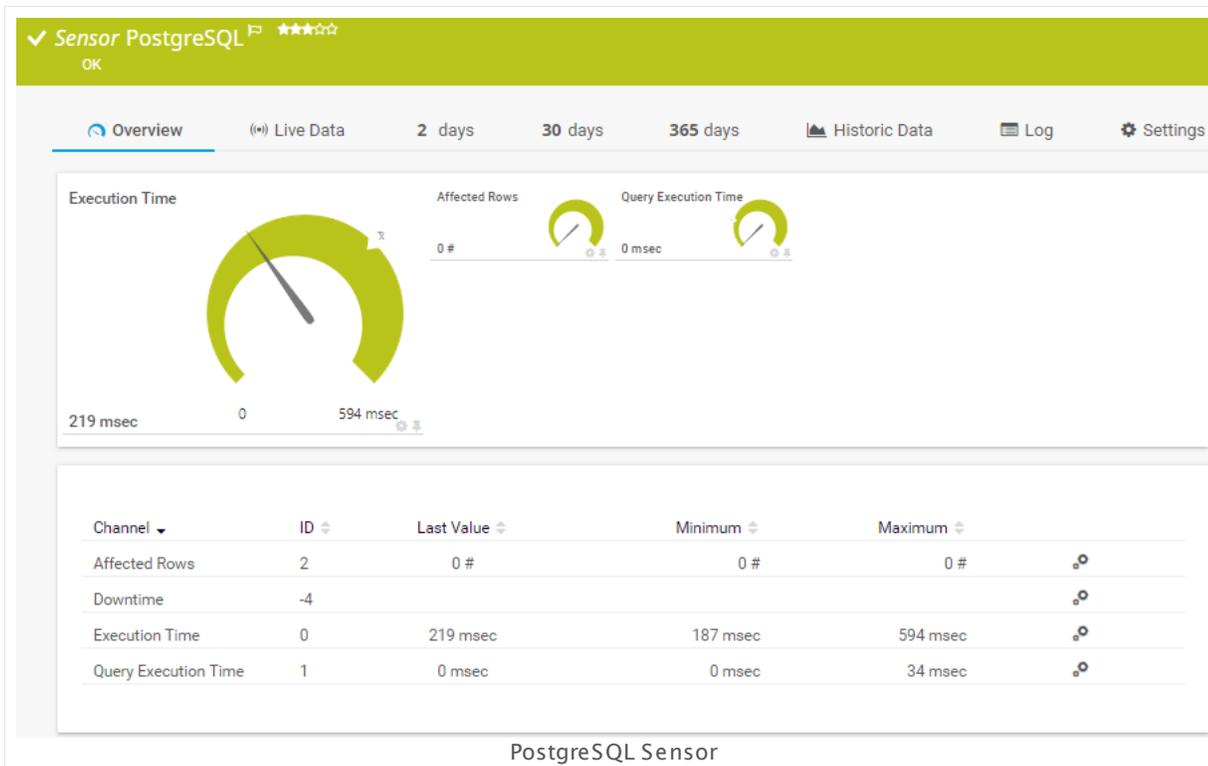
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.102 PostgreSQL Sensor

The PostgreSQL sensor monitors a database on a PostgreSQL server and executes a defined query.

It can show the following:

- Execution time of the whole request (including connection buildup, query execution, transaction handling, disconnection)
- Execution time of a given query
- Number of rows that were addressed by the query (including `select` statements if you process data tables)
- It can also process the data table and show defined values in individual channels.



Remarks

- [Requires](#) ¹⁵⁷⁵ .NET 4.5 or later on the probe system.
- Define credentials, custom port (if required), and timeout in settings section [Credentials for Database Management Systems](#) ⁴¹³ of the parent device, or in the settings of a group or probe above.
- Your SQL query must be stored in a file on the system of the probe the sensor is created on. If you use it on a remote probe, store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.

- Save the SQL script with the query into the `\Custom Sensors\sql\postgresql` subfolder of your PRTG installation. See manual section [Data Storage](#)^[3734] for more information about how to find this path
- This sensor type supports PostgreSQL 7.x or later.
- PRTG Manual: [Monitoring Databases](#)^[3534] (includes an [example](#)^[3535] for channel value selection)
- Knowledge Base: [How can I monitor strings from an SQL database and show a sensor status depending on it?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATABASE SPECIFIC

Database	Enter the name of the PostgreSQL database to which the sensor connects (for example, MyDatabase). This is a logical entity on the database server where database objects like tables or stored procedures exist.
SSL Mode	<p>Select the PostgreSQL SSL mode for the sensor connection. PostgreSQL SSL connections require OpenSSL to be installed on both the target server and on the PRTG probe system with this sensor.</p> <p>The SSL mode options you can choose here are the same as the values of the PostgreSQL sslmode parameter. PRTG sends it with the sensor requests.</p> <p>Choose between these SSL modes:</p>

DATABASE SPECIFIC

- **Disable**
- **Allow**
- **Prefer**
- **Require**

 For details about the PostgreSQL SSL modes, refer to the PostgreSQL documentation.

DATA

SQL Query File

Select an SQL script file that includes a valid SQL statement to execute on the server. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

The script will be executed with every scanning interval. The list contains SQL scripts from the database management system specific **\Custom Sensors\sql** subfolder of your PRTG installation. Store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node!

 For more information on how to find this path, see section [Data Storage](#)³⁷³⁴. By default, there is the demo script **Demo Serveruptime.sql** available that you can use to monitor the uptime of the target server.

For example, a correct expression in the file could be: **SELECT AVG (UnitPrice) FROM Products**. If you want to use transactions, separate the individual steps with semicolons ";".

 Please be aware that with each request, the full result set will be transferred, so use filters and limits in your query.

 See also this Knowledge Base article: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)

SQL Variables

You can use the following variables in your query file to have them replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

DATA

- Microsoft SQL, MySQL, PostgreSQL: **@prtg**
- Oracle SQL: **:prtg**
- ADO SQL: **?** (question mark)

@prtg, **:prtg**, and **?** behave like common SQL variables, so consider the general rules for SQL variables. For example, you cannot use a variable for a table in the FROM statement of a query.

Example for variables usage: **SELECT * FROM Table WHERE @prtg**

Use Input Parameter

Define if you want to pass a parameter to your SQL query file. This will replace the variables **@prtg** (Microsoft SQL, MySQL, PostgreSQL), or **:prtg** (Oracle SQL), or **?** (ADO SQL) in the SQL query, considering the general rules for SQL variables. Choose between:

- **Don't use input parameter (default):** Execute the SQL query file without using variables.
- **Use input parameter:** Execute an SQL query file that contains a variable. Provide the parameter you want to use in the query below.

Input Parameter

This field is only visible if you choose **Use input parameter** above. Enter the parameter you want to pass to the SQL query file. This parameter will replace the variable **@prtg** or **:prtg** or **?** in the SQL query, considering the general rules for SQL variables.

You can also use PRTG placeholders for custom sensors (command line parameters) as input parameter, for example, **%sensorid** or **%deviceid**. For details, see section [Custom Sensors](#)^[365].

 Provide strings as they are and do not surround them with quotation marks. PRTG will correctly insert string parameters into the query automatically.

Use Transaction

Define if you want to use transactions and if they will affect the database content. Choose between:

- **Don't use transaction (default):** No transactions will be executed.
- **Use transaction and always rollback:** Choose this option to ensure that no data in the database will be changed by the query. In the SQL query file, separate the single steps of the transaction with semicolons.
- **Use transaction and commit on success:** Choose this option to perform changes on the database with the query. The changes will only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.

DATA

Data Processing

Define if you want to process data from the database. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- **Just execute the query:** If you select this option, the sensor will only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed somehow with the query (for example, created, deleted, edited).
- **Count table rows:** Choose this option if you perform a **SELECT** statement and want to monitor how many rows of the data table this statement returns.
- **Process data table:** Select this option to read and analyze the queried data table. If you select this option, the sensor will count rows with **SELECT** statements as well.

Handle DBNull in Channel Values as

This setting is only visible if you select **Process data table** above. Define the sensor behavior if **DBNull** is returned by the query. Choose between:

- **Error:** The sensor will show a **Down** status if **DBNull** is reported.
- **Number 0:** The sensor will recognize the result **DBNull** as a valid value and interpret it as the number **0**.

Select Channel Value by

This setting is only visible if you select **Process data table** above. Define how the desired cell in the database table will be selected. This is necessary to configure the cells that will be used in the sensor channels. Choose between:

- **Column number:** The channel value will be determined by using the value in row 0 of the column whose number you specify below.
- **Column name:** The channel value will be determined by using the value in row 0 of the column whose name you specify below.
- **Row number:** The channel value will be determined by using the value in column 0 of the row whose number you specify below.
- **Key value pair:** The channel value will be determined by searching in column 0 for the key you specify below and returning the value in column 1 of the same row where the key value was found.

The option you choose here also defines the method to optionally determine a value for the sensor message. For details, see setting **Use Data Table Value in Sensor Message** below.

DATA

 See manual section [Monitoring Databases](#)  for an [example](#)  for channel value selection.

Sensor Channel #x This setting is only visible if you select **Process data table** above. You can define up to 10 different channels for the data processing of this sensor. You have to define at least one data channel if you process the data table, so you will see all available settings for **Channel #1** without enabling it manually. For all other possible channels, choose between:

- **Disable:** This channel will not be added to the sensor.
- **Enable:** This channel will be added to the sensor. Define the settings as described above.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name This setting is only visible if you select **Process data table** above. Enter a unique name for the channel. Please enter a string. Channels will be generated dynamically with this name as identifier. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Column Number This setting is only visible if you select **Column number** above. Provide the number of the column that will be used to determine the channel value in row 0. Please enter an integer value.

Sensor Channel #x Column Name This setting is only visible if you select **Column number** above. Provide the name of the column that will be used to determine the channel value in row 0. Please enter a string.

Sensor Channel #x Row Number This setting is only visible if you select **Row number** above. Provide the number of the row that will be used to determine the channel value in column 0. Please enter an integer value.

Sensor Channel #x Key This setting is only visible if you select **Key value pair** above. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found will be used to determine the channel value. Please enter a string.

Sensor Channel #x Mode This setting is only visible if you select **Process data table** above. Define how to display the determined value in the channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

DATA

- **Absolute (recommended):** Shows the value as the sensor retrieves it from the data table.
- **Difference:** The sensor calculates and shows the difference between the last and the current value returned from the data table. This mode is not compatible with the unit **Value Lookup**.

Sensor Channel #x
Unit

This setting is only visible if you select **Process data table** above. Define the unit of the channel value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile
- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#).

 To use [lookups](#) with this channel, choose **Value Lookup** and select your lookup file below. Do not use **Custom** for using lookups with this sensor!

 Using the unit **Value Lookup** is not possible when you choose the **Difference** mode. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit

This setting is only visible if you select **Custom** above. Define a unit for the channel value. Please enter a string.

DATA

Sensor Channel #x Value Lookup	This settings is only visible if you select Value Lookup above. Select a lookup <small>3693</small> file that you want to use with this channel.
Use Data Table Value in Sensor Message	<p>This setting is only visible if you select Process data table above. Define if the sensor message will show a value from the data table. Choose between:</p> <ul style="list-style-type: none"> ▪ Disable: Do not use a custom sensor message. ▪ Enable: Define a custom sensor message with a defined value of the data table. Define the value selection below. <p>The method to determine a value for the sensor message is defined in setting Select Channel Value by above.</p>
Sensor Message Column Number	<p>This setting is only visible if you select Column number and Use Data Table Value in Sensor Message above. Enter the number of a column. The sensor message will show the value in row 0 of this column. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Column Name	<p>This setting is only visible if you select Column name and Use Data Table Value in Sensor Message above. Enter the name of a column. The sensor message will show the value in row 0 of this column. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Row Number	<p>This setting is only visible if you select Row number and Use Data Table Value in Sensor Message above. Enter the number of a row. The sensor message will show value in column 0 of this row. Please enter an integer value.</p> <p> Columns and rows start with index 0.</p>
Sensor Message Key	<p>This setting is only visible if you select Key value pair and Use Data Table Value in Sensor Message above. Enter a key to search for in column 0 of the data table. The sensor message will show the value in column 1 of the row where the key has been found. Please enter a string.</p> <p> Columns and rows start with index 0.</p>
Sensor Message	<p>This setting is only visible if you select Use Data Table Value in Sensor Message above. Define the sensor message. Please enter a string. Use the placeholder {0} at the position where the value will be added.</p>

DATA

Example: **The message is {0}**

If Sensor Message Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³⁷⁷⁰ whenever the sensor value changes.

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?

- <https://kb.paessler.com/en/topic/63259>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.103 Probe Health Sensor

The Probe Health sensor monitors internal PRTG parameters. It shows the status of the PRTG probe (either for the local probe, the hosted probe, a [remote probe](#), or a [cluster](#) probe).

It checks various parameters of your PRTG system that can affect the quality of the monitoring results:

- **Health:** This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Probe Process CPU Load:** This channel shows the current percentage CPU load that the probe process causes. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value usually should stay below 50%.
- **Data Storage Free:** This channel shows the free disk space on the probe system. PRTG dynamically sets limits for this channel. You can manually override these limits in the [sensor channel settings](#).
- **Handles:** This is a counter for the data structures of the operating system. It is responsible for internal resource management. Repeated obviously increasing values should be investigated.
- **Interval Delay non-WMI&SNMP:** This channel shows the percentage interval delay for all sensor types that are not of the type SNMP or WMI. If this value is over 0%, try to increase the [scanning intervals](#) or distribute your sensors over [multiple probes](#).
- **Interval Delay SNMP:** This channel shows the percentage interval delay for SNMP sensors. If this value is above 0%, there are probably too many very slow SNMP V3 sensors. In this case, try to increase the [monitoring intervals](#) or distribute the sensors over [several probes](#).
- **Interval Delay WMI:** This channel shows the percentage interval delay for WMI sensors. If this value is above 0%, WMI sensors could not check the target device according to their interval. 100% means that WMI sensors on the average are checked with twice their interval. For values above 0% try to increase the [monitoring intervals](#) or distribute the sensors over [several probes](#) to keep the number of WMI sensors per probe below 120 (with 60 seconds interval) or 600 (with 300 seconds interval).
- **Lost Flow Packets:** This channel shows the percentage of lost [flow](#) packets. The higher this value, the less flow packages PRTG can handle. Usually, this value should be 0%. Investigate increasing values.
- **Memory Usage:** This channel shows the amount of memory being used by the PRTG probe service as reported by the memory manager. Repeated obviously increasing values should be investigated. If the value is constantly above 2 GB this indicates that PRTG runs at its limits. In this case you should distribute some sensors to [Remote Probe](#).
- **Message Queue:** This channel shows the number of monitoring results from the probe that have not been processed yet by the core. This value usually should stay below 1/10 of the sensor count.
- **Open Requests:** This channel shows the number of currently active monitoring requests. This value should stay below the maximum of 500 open requests.
- **Syslog Buffer:** This channel shows the number of buffered syslog packages. Usually, this value should be 0 (or very low). Investigate increasing values.

- **Threads:** This channel shows the number of program parts that are running simultaneously currently. This value can increase with heavy load. The number should not exceed 100 in normal operation.
- **Toplist Memory:** This channel shows the amount of RAM that the [Toplists](#) on this probe are using. Stay below 1 GB memory usage (depending on available memory on the probe system). If necessary, reduce the number of toplist or distribute them on [multiple probes](#).
- **Trap Buffer:** This channel shows the number of buffered SNMP traps. Usually, this value should be 0 (or very low). Investigate increasing values.



Sensor in Other Languages

Dutch: **Probe Status**, French: **État de la probe**, German: **Zustand der Probe**, Japanese: ? ? ? ? ? , Portuguese: **Funcionamento da sonda**, Russian: **Работоспособность зонда**, Simplified Chinese: ? ? ? ? ? ? , Spanish: **Salud de sonda**

Remarks

- PRTG creates this sensor automatically and you cannot delete it.

- You can create this sensor only on a probe device (either local probe, a [remote probe](#), or a [cluster](#) probe).
- Knowledge Base: [My probe system is running out of disk space. What can I do?](#)

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My probe system is running out of disk space. What can I do?

- <https://kb.paessler.com/en/topic/64628>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

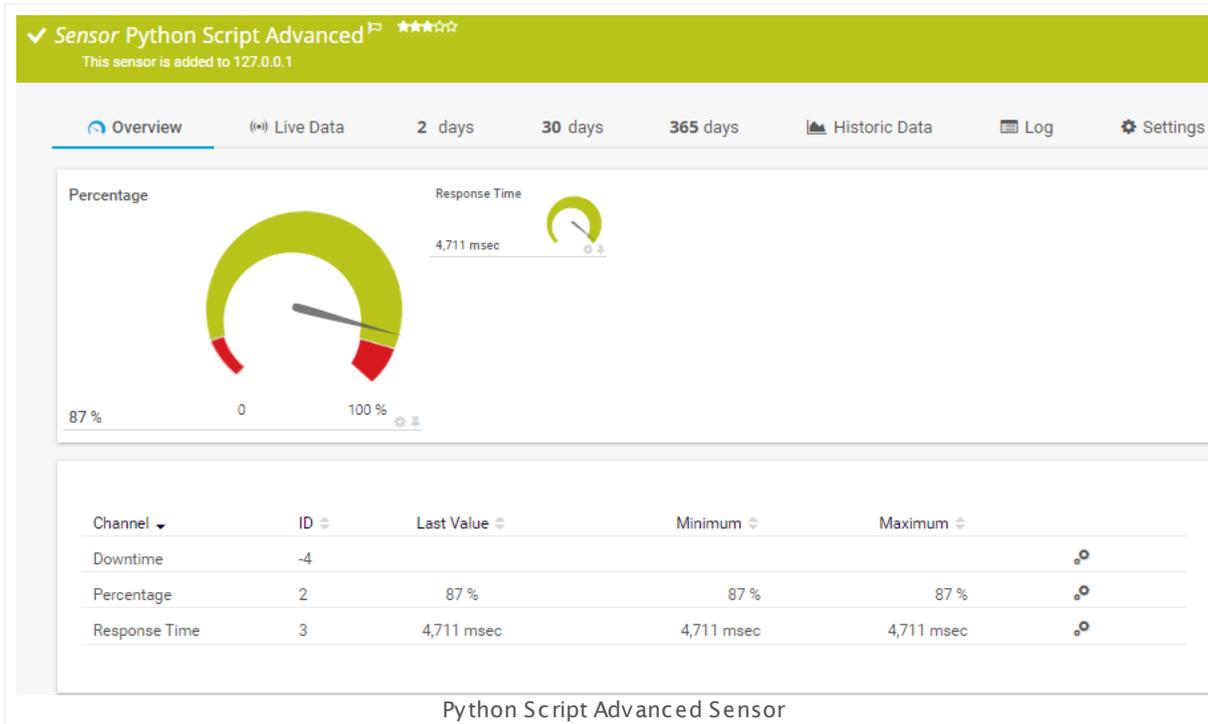
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.104 Python Script Advanced Sensor

The Python Script Advanced sensor executes a Python script on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API). The return value of this sensor must be valid JSON or XML.

- The sensor can show values returned by the Python script in multiple channels.



Sensor in Other Languages

Dutch: **Python Script Geavanceerd**, French: **Paramètres du capteur avancé**, German: **Python-Skript (Erweitert)**, Japanese: **Python ? ? ? ? ? (? ?)**, Portuguese: **Script Python Avançado**, Russian: **Настройки расширенного сенсора**, Simplified Chinese: **Python ? ? ? ?**, Spanish: **Secuencia de comandos Python avanzada**

Remarks

- You must store the script file on the system of the probe where you create the sensor: If used on a remote probe, you must store the file on the system running the remote probe. In a cluster setup, copy the file to every cluster node.
- For best sensor usage, we recommend that the return value is JSON encoded.
- The timeout of the sensor is its [scanning interval](#) minus 1 second. Ensure your Python script does not run longer than this.
- Print commands in the Python script are not supported and lead to an invalid JSON result.
- Exceptions in the script are not supported.
- Sensor channel values greater than 2^{62} are not supported.

- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
 - This sensor [does not support more than 50 channels](#) ¹⁵⁹⁸ officially.
 - Knowledge Base: [What is the Mutex Name in PRTG's EXE/Script Sensor's settings?](#)
 - Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Python Script

Select a Python script from the list. The sensor will execute it with every [scanning interval](#) ¹⁶⁰².

This list shows all Python script files available in the **\Custom Sensors\python** subdirectory of the probe system's PRTG program directory (see [Data Storage](#) ³⁷³⁴). For the files to appear in this list, please store the files into this folder ending in **.py**. To show the expected values and sensor status, your files must return the expected XML or JSON format to standard output. Values and message must be embedded in the XML or JSON. We recommend JSON encoded return values.



For detailed information on how to build custom sensors and for the expected return format, see section [Custom Sensors](#) ³⁶⁴⁷.



 When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Python Script	Shows the Python script file that the sensor executes with each scan as defined at sensor creation. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Security Context	Define the Windows user account that the sensor uses to run the Python interpreter. Choose between: <ul style="list-style-type: none">▪ Use security context of probe service: Run the selected file under the same Windows user account the probe is running on. By default, this is the Windows system user account (if not manually changed).▪ Use Windows credentials of parent device: Use the Windows user account defined in the settings of the parent device on which you create this sensor. Please navigate to the parent device settings^[402] of this sensor to change these Windows credentials.
Device Credentials	Define if you want to transmit device credentials to the Python script. PRTG adds the device credentials to the JSON object that is passed to the script as command line parameter. Please navigate to parent device settings ^[402] of this sensor to change these credentials. Choose between: <ul style="list-style-type: none">▪ Do not transmit device credentials: No device credentials are given to the script.▪ Transmit Windows credentials: Windows credentials^[407] are given to the script.▪ Transmit Linux credentials: Linux credentials^[408] are given to the script.▪ Transmit SNMP credentials: SNMP credentials^[411] are given to the script.▪ Transmit all device credentials: Windows, Linux, and SNMP credentials are all given to the script. <p> All parameters are transmitted in plain text.</p>
Additional Parameters	Define additional parameters to add to the JSON object that is passed to the script as command line parameter. Please enter a string or leave the field empty. <p> All parameters are transmitted in plain text.</p>

SENSOR SETTINGS

Mutex Name Define any desired mutex name for the process. All script sensors having the same mutex name will be executed serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running simultaneously. Please enter a string or leave the field empty.

 For more details, please see this Knowledge Base article: [What is the Mutex Name in PRTG's EXE/Script Sensor's settings?](#)

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

 You can use **Write sensor result to disk** to inspect the passed JSON object that contains all parameters (PRTG on premises only). This way you can find out which key you can access when you script.

 Transmitted passwords are masked in the logfile.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What is the Mutex Name in PRTG's EXE/Script Sensor's settings?

- <https://kb.paessler.com/en/topic/6673>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

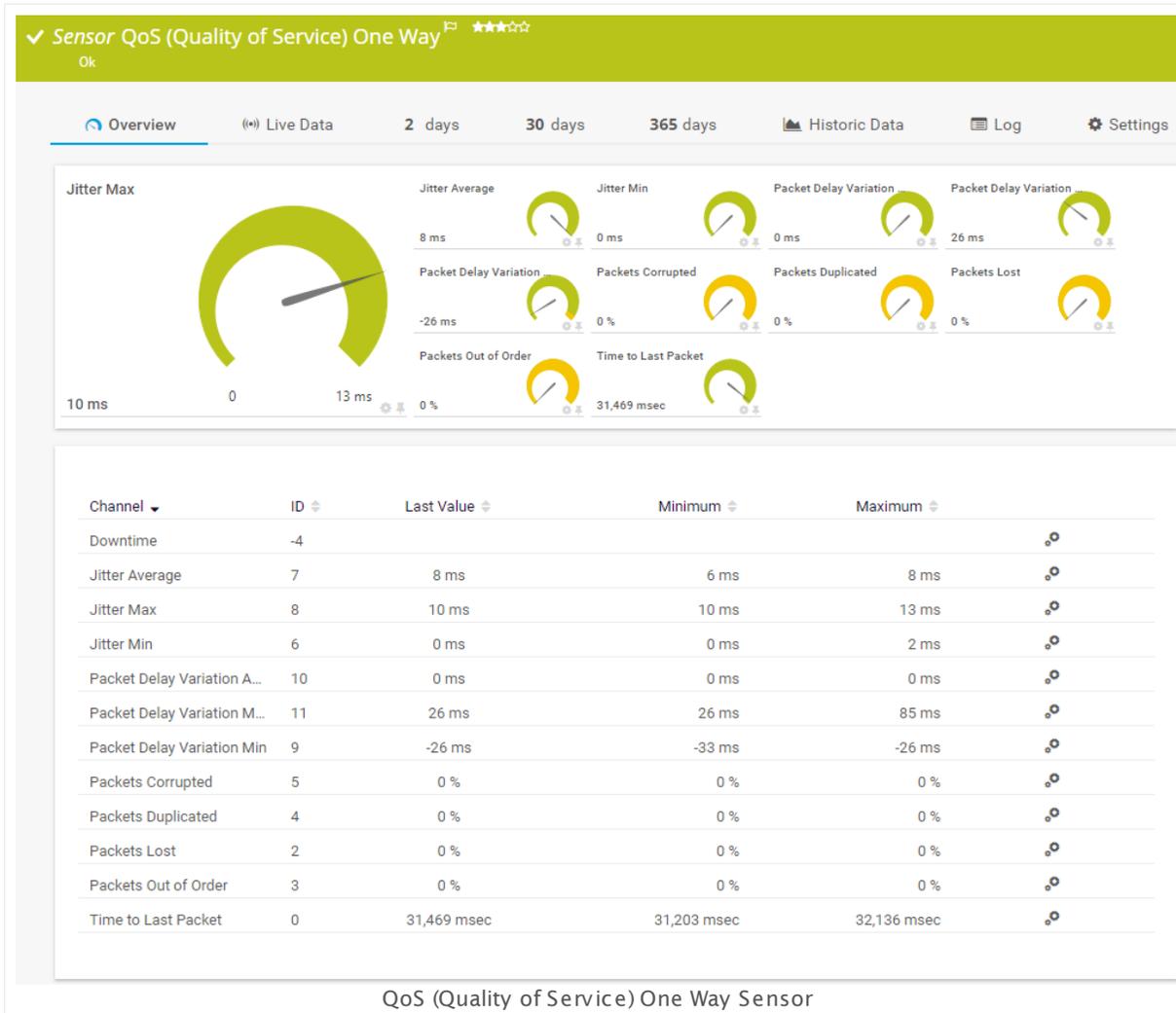
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.105 QoS (Quality of Service) One Way Sensor

The QoS (Quality of Service) One Way sensor monitors parameters regarding the quality of a network connection between two probes. This is important, for example, when using Voice over IP (VoIP) over this connection.

The sensor sends a series of UDP packets from the parent probe to another probe and measures these parameters:

- Jitter in milliseconds (maximum, minimum, average)
- Packet delay variation in milliseconds (maximum, minimum, average)
- Corrupted packets in percent
- Duplicated packets in percent
- Lost packets in percent
- Packets out of order in percent
- Time to last packet in milliseconds



Sensor in Other Languages

Dutch: **QoS (Quality of Service) Eén Richting**, French: **QoS (Quality of Service) à sens unique**, German: **QoS (Quality of Service) Unidirektional**, Japanese: **QoS (Quality of Service) Unidirectional**, Portuguese: **QoS (Qualidade de serviço) Unidirecional**, Russian: **Одностороннее качество обслуживания**, Simplified Chinese: **QoS (Quality of Service) 单向**, Spanish: **QoS (Quality of Service) unidireccional**

Remarks

- You have to configure at least one [remote probe](#) in your PRTG on premises setup for this sensor to work, and at least two remote probes in PRTG hosted by Paessler.
- You can create this sensor on the Probe Device of either a local or remote probe.
- For a general introduction to the technology behind Quality of Service monitoring, please see manual section [Monitoring Quality of Service](#).

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QUALITY OF SERVICE MEASUREMENT

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Target Probe	<p>Define the target probe that will receive the UDP packets. The dropdown menu shows all local and remote probes in your setup.</p> <p>When running the sensor on the PRTG on premises local probe, select a remote probe as Target Probe. If no remote probe is available, please install and connect a remote probe^[3707] first. When running the sensor on a remote probe, select either another remote probe or the local probe in PRTG on premises as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe.</p> <p> You must ensure that firewalls, NAT rules, etc. allow UDP packets to reach the target probe. The Windows firewall on the target system will be opened automatically by the probe.</p> <p> In PRTG hosted by Paessler you can only select another remote probe as target probe. QoS measurements for connections to the hosted probe are not possible.</p>
Target Host/IP	Define the IP address of the target probe to which the probe the sensor is created on connects. If you do not use NAT rules, this is usually the address shown above next to the target probe's name.
Port	<p>Define the source and target port for the UDP packets. This port is used on both the source and target probe. Use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536.</p> <p> This port must be available on both the source and target system.</p>
Number of Packets	Define how many packets the sensor sends with each scanning interval. Please enter an integer value. Default value is 1000 . We recommend that you use the default value.
Size of Packets (Bytes)	Define the size in bytes of the packets that the sensor sends. Please enter an integer value. Default value is 172 . We recommend that you use the default value.
Time between Packets (ms)	Define the time in milliseconds that the sensor waits between two packets. Please enter an integer value. Default value is 20 . We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.106 QoS (Quality of Service) Round Trip Sensor

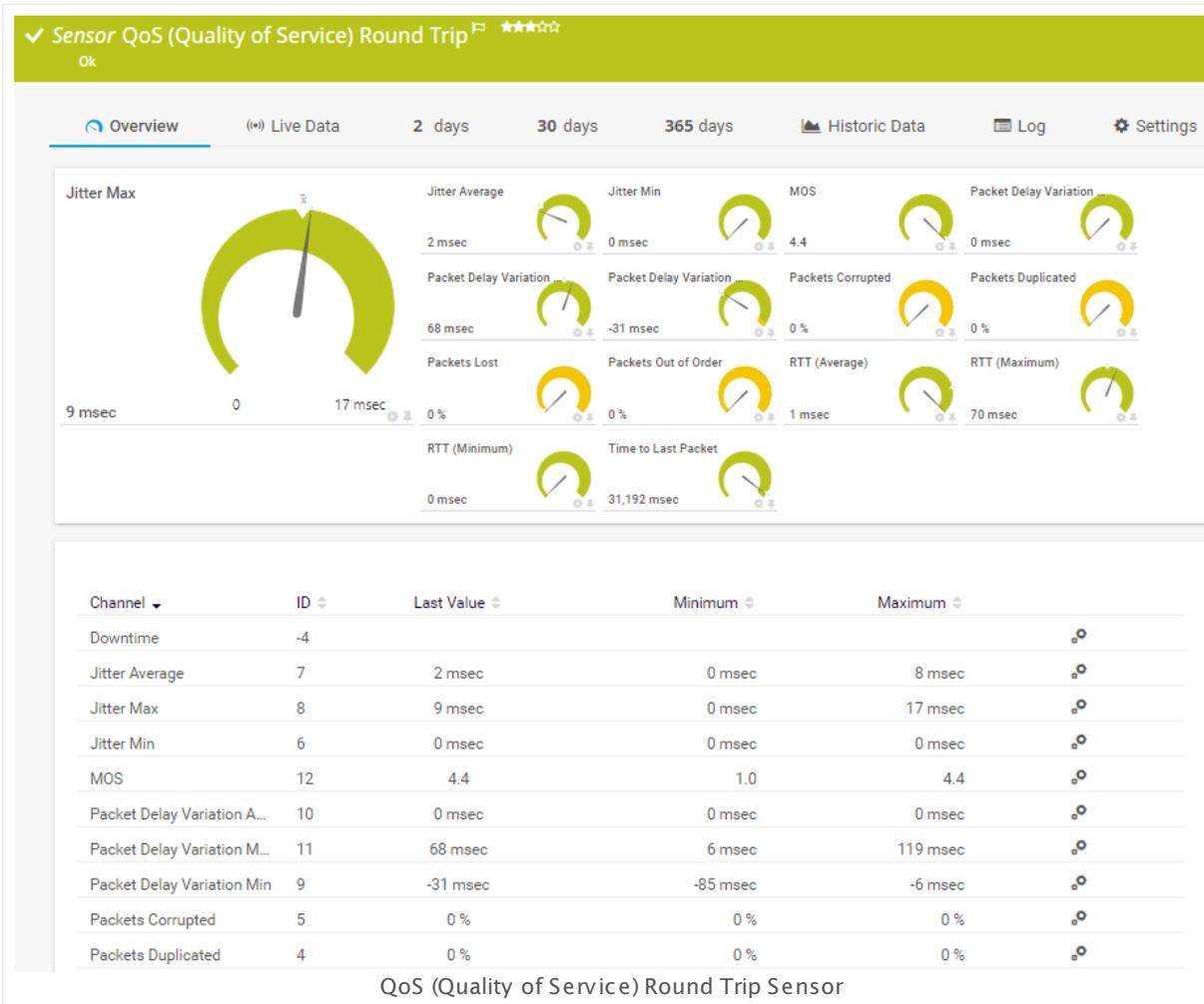
The QoS (Quality of Service) Round Trip sensor monitors parameters regarding the quality of a network connection between two probes. This is important, for example, when using Voice over IP (VoIP) over this connection.

The sensor sends a series of UDP packets from the source probe to a target at the 'end' of the connection line. Then, the packets are sent back to the original probe ("round trip").

The sensor measures the following parameters:

- Jitter in milliseconds (maximum, minimum, average)
- Packet delay variation in milliseconds (maximum, minimum, average)
- MOS (Mean Opinion Score)
- Corrupted packets in percent
- Duplicated packets in percent
- Lost packets in percent
- Packets out of order in percent
- Round trip time (RTT) in milliseconds (maximum, minimum, average)
- Time to last packet in milliseconds

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 106 QoS (Quality of Service) Round Trip Sensor



QoS (Quality of Service) Round Trip Sensor

Sensor in Other Languages

Dutch: **QoS (Quality of Service) Heen en weer**, French: **Aller-retour du QoS (Quality of Service)**, German: **QoS (Quality of Service) Round Trip**, Japanese: **QoS (Quality of Service)**, Portuguese: **QoS (Qualidade de serviço) Ida e volta**, Russian: **Цикл тестирования качества обслуживания**, Simplified Chinese: **QoS (Quality of Service) Round Trip**, Spanish: **QoS (Calidad de servicio) Round Trip**

Remarks

- You have to configure at least one [remote probe](#) in your PRTG on premises setup and at least two remote probes in PRTG hosted by Paessler, or you need to set up the **PRTG QoS Reflector** tool on the target machine at the endpoint of the monitored connection.
- Knowledge Base: [How can I monitor QoS roundtrips without using remote probes?](#)
- Knowledge Base: [How does PRTG calculate the MOS score for QoS sensors?](#)
- Knowledge Base: [What connection settings are necessary for the QoS \(Quality of Service\) Round Trip Sensor?](#)

- For a general introduction to the technology behind Quality of Service monitoring, please see manual section [Monitoring Quality of Service](#).
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QUALITY OF SERVICE MEASUREMENT

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

QoS Target Define the type of target that will receive the UDP packets. Choose between:

- **PRTG Probe (recommended):** The connection endpoint is a PRTG probe.
- **Custom Target:** Choose this option if you want to use the **PRTG QoS Reflector** as connection endpoint.

 For more information about the QoS Reflector, see this Knowledge Base: [How can I monitor QoS roundtrips without using remote probes?](#)

Target Probe This setting is only available if you select PRTG probe as QoS target. In the dropdown menu, you see all local and remote probes of your setup.

When running the sensor on the PRTG on premises local probe, select a remote probe as **Target Probe**. If no remote probe is available, [install and connect a remote probe](#) first or use the **PRTG QoS Reflector**.

When running the sensor on a remote probe, select either another remote probe or the local probe in PRTG on premises as target. The sensor will measure values for the network track between the probe the sensor is created on and the target probe.

 You must ensure that firewalls, NAT rules, etc. will allow the UDP packets to reach the target probe. The Windows firewall on the target system will be automatically opened by the probe. For details, see this Knowledge Base article: [What connection settings are necessary for the QoS \(Quality of Service\) Round Trip Sensor?](#)

 In PRTG hosted by Paessler you can only select another remote probe as target probe. QoS measurements for connections to the hosted probe are not possible.

QUALITY OF SERVICE MEASUREMENT

Target Host/IP	<p>Define the IP address of the QoS target. If you use the QoS Reflector, enter the address of the machine on which the reflector script runs. If you use a probe, enter the address of the probe to which the probe the sensor is created on connects.</p> <p> If you do not use NAT rules, this is usually the address shown above next to the target probe's name.</p>
Port	<p>Define the source and target port for the UDP packets. This port will be used on both the source and target probe. Use a different port for each QoS sensor to make sure packets can be assigned correctly. Enter an integer value between 1024 and 65536.</p> <p> This port must be available on both the source and target system.</p>
Number of Packets	<p>Define how many packets the sensor sends for each scanning interval. Please enter an integer value. Default value is 1000. We recommend that you use the default value.</p>
Size of Packets (Bytes)	<p>Define the size in bytes of the packets that the sensor sends. Please enter an integer value. Default value is 172. We recommend that you use the default value.</p>
Time between Packets (ms)	<p>Define the time in milliseconds that the sensor waits between two packets. Please enter an integer value. Default value is 20. We recommend that you use the default value.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How does PRTG calculate the MOS score for QoS sensors?

- <https://kb.paessler.com/en/topic/59491>

Knowledge Base: How can I monitor QoS roundtrips without using remote probes?

- <https://kb.paessler.com/en/topic/61176>

Knowledge Base: What connection settings are necessary for the QoS (Quality of Service) Round Trip Sensor?

- <https://kb.paessler.com/en/topic/65410>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

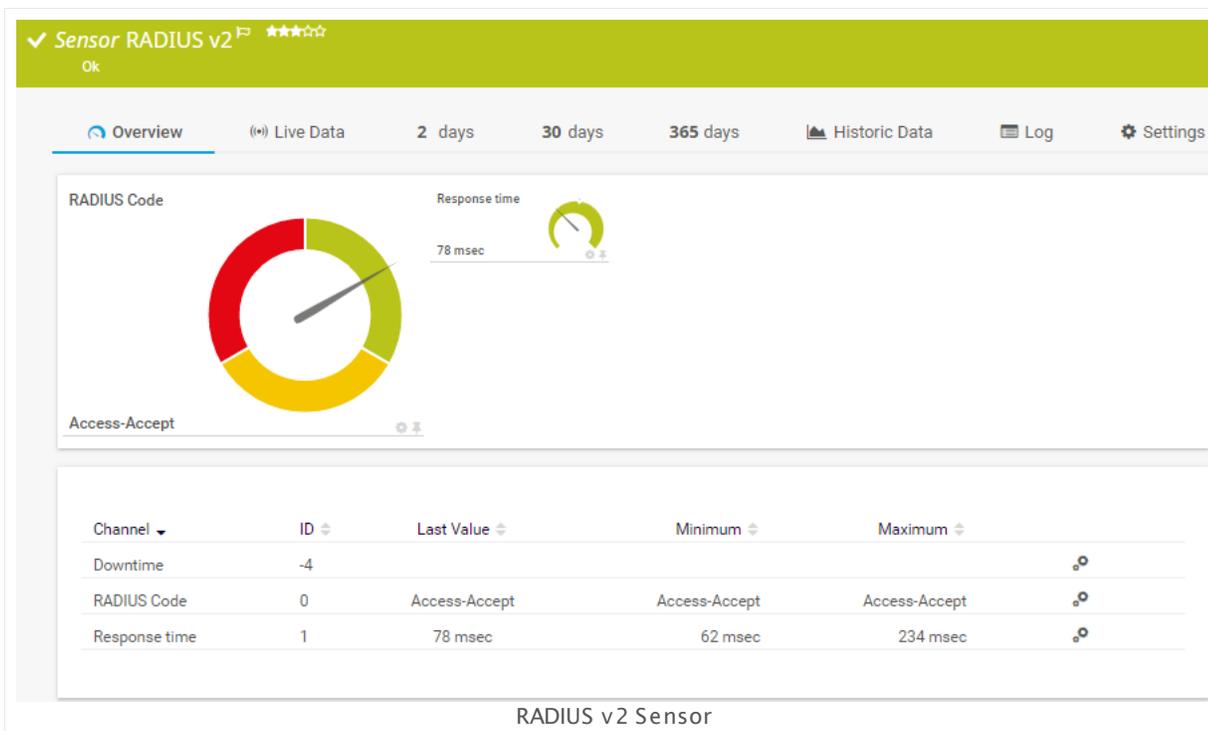
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.107 RADIUS v2 Sensor

The RADIUS v2 sensor monitors a Remote Authentication Dial-In User Service (RADIUS) server according to [RFC 2865](#). The sensor tries to authenticate at the server and shows the following:

- Response time
- RADIUS code:
 - Access-Accept ([sensor status](#)¹⁹⁵ Up)
 - Access-Challenge (Warning)
 - Access-Reject (Down)
- If authentication fails, the sensor will show a **Down status**¹⁹⁵.



Remarks

- [Requires](#)¹⁶²⁹ .NET 4.5 on the probe system.
- This sensor only supports plain text authentication (Password Authentication Protocol (PAP)).
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

RADIUS SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value, the request is aborted and an error message is triggered. The maximum value is 900 seconds (15 minutes). Please enter an integer value.
User	Enter the username that is used for authentication at the RADIUS server. Please enter a string.
Password	Enter the password that is used for authentication between the client (this is the PRTG probe on which the sensor runs) and the RADIUS server. Please enter a string.
Secret	Enter the shared secret that is used for authentication between the authenticator (this is the PRTG probe) and the RADIUS server. Please enter a string.
Port	Enter the port number that is used for the connection to the RADIUS server. The default value is 1812 . Please enter an integer value.
Network Access Server	Define how to identify the Network Access Server (NAS) . Choose between: <ul style="list-style-type: none"> ▪ Use NAS IP address: Enter the IP address for identification below. ▪ Use NAS identifier: Enter the identifier below.
NAS IP Address	This field is only visible if you select Use NAS IP address as an identification method above. Enter a valid IP address for the Network Access Server (NAS) that originates the access request.
NAS Identifier	This field is only visible if you select Use NAS identifier above. Enter an identifier for the NAS that originates the access request.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> ▪  For more information on how to find the folder used for storage, see section Data Storage ³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

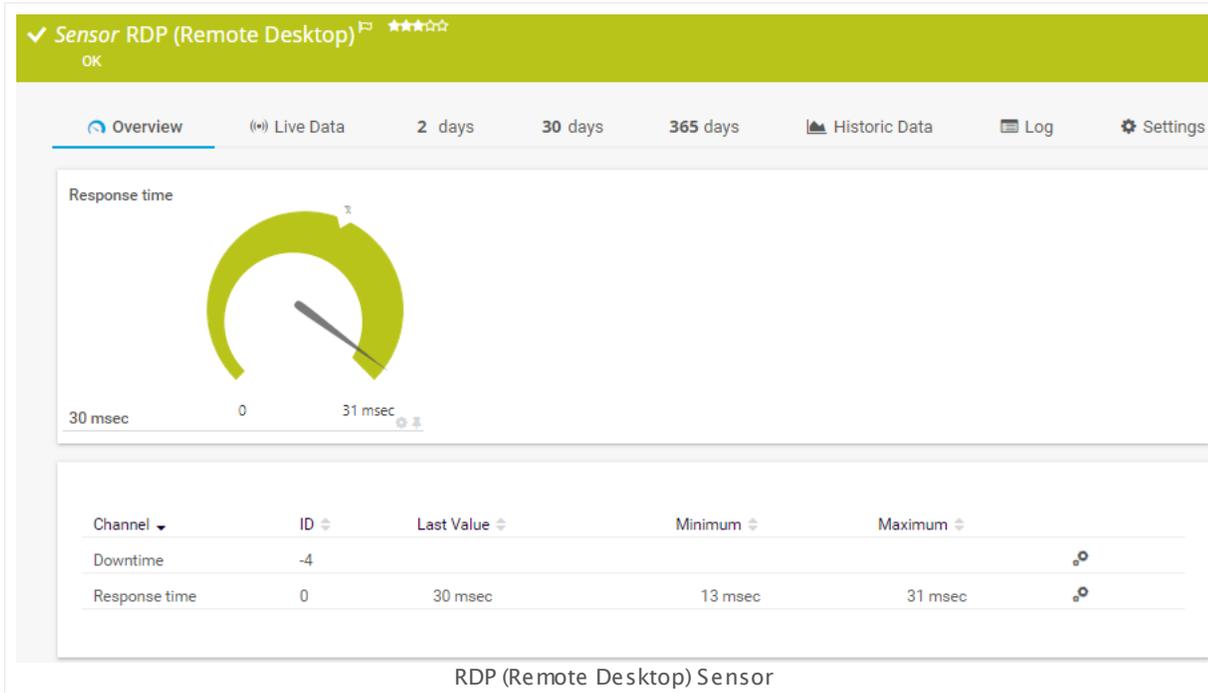
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.108 RDP (Remote Desktop) Sensor

The RDP (Remote Desktop) sensor monitors remote desktop services (RDP, Terminal Services Client).

- It shows the response time of the service.



Sensor in Other Languages

Dutch: **RDP (Remote Desktop)**, French: **RDP (Bureau à distance)**, German: **RDP (Remote Desktop)**, Japanese: **RDP (? ? ? ? ? ? ? ? ?)**, Portuguese: **RDP (desktop remoto)**, Russian: **RDP (удаленный рабочий стол)**, Simplified Chinese: **RDP (? ? ? ?)**, Spanish: **RDP (Escritorio remoto)**

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value. Default value is 3389 . We recommend that you use the default value.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Does PRTG impair my Citrix environment?

- <https://kb.paessler.com/en/topic/61880>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.109 REST Custom Sensor

The REST Custom sensor queries a REST Application Programming Interface (API) endpoint and maps the JSON or XML result to sensor values. The mapping rule has to be available as a REST configuration file in JSON template (*.template) format according to the PRTG API definition for custom sensors.

- The sensor can show values returned by a REST API in multiple channels.

For details about the return value format, see section [Custom Sensors](#) ³⁶⁴¹.

✓ Sensor REST Custom ★★★★☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Response Time



7 msec 0 425 msec

content.compressionP...

50 #

content.currentPower

965 #

content.health.value

5 #

content.id

0 #

content.sizeFree

3.345.678 #

content.sizeSubscribed

1.345.678 #

content.sizeTotal

12.345.678 #

content.sizeUsed

1.345.678 #

Channel	ID	Last Value	Minimum	Maximum	
content.compressionPer...	9	50 #	50 #	50 #	🔍
content.currentPower	5	965 #	965 #	965 #	🔍
content.health.value	3	5 #	5 #	5 #	🔍
content.id	2	0 #	0 #	0 #	🔍
content.sizeFree	7	3.345.678 #	3.345.678 #	3.345.678 #	🔍
content.sizeSubscribed	4	1.345.678 #	1.345.678 #	1.345.678 #	🔍
content.sizeTotal	6	12.345.678 #	12.345.678 #	12.345.678 #	🔍
content.sizeUsed	8	1.345.678 #	1.345.678 #	1.345.678 #	🔍
Downtime	-4				🔍
Response Time	0	7 msec	1 msec	425 msec	🔍

REST Custom Sensor

Sensor in Other Languages

Dutch: **REST Aangepast**, French: **REST personnalisé**, German: **REST (Benutzerdef.)**,
 Japanese: **REST ? ? ?**, Portuguese: **REST (Customizado)**, Russian: **Специальные настройки REST**,
 Simplified Chinese: **REST ? ? ?**, Spanish: **REST personalizado**

Remarks

- The REST configuration file that contains the mapping rules must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- This sensor [does not support more than 50 channels](#)¹⁶⁴⁷. If you have more than 50 channel mappings in your REST configuration file, the sensor will show an error.
- In a cluster, status changes triggered by limits only work on the master node.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

REST SPECIFIC

REST Configuration	<p>Select a REST configuration from the list. The sensor will use it to map the JSON or XML result from the REST query into sensor values.</p> <p>Default is channelDiscovery. If you choose this REST configuration, the sensor will parse the returned JSON or XML and automatically create channels based on available values: one channel for each number and boolean, for strings if they are convertible into numbers.</p> <p>This list shows all available files in the <code>\Custom Sensors\rest</code> sub-directory of the probe system's PRTG program directory (see Data Storage³⁷²⁴). To appear in this list, store the files as JSON template (*.template) into this folder.</p>
--------------------	---

REST SPECIFIC

 Using custom scripts is not possible on hosted probes. To use custom REST configurations, add this sensor to a remote probe instead and save the file on this system.

To show the expected values and sensor status, your files must return the expected JSON format. Channels, values, and messages must be embedded in valid JSON using JSONPath. For details, see section [Define Sensor Channels and Select Channel Values](#) ^[1658].

 For detailed information on how to build custom sensors and for the expected return format, see section [Custom Sensors](#) ^[3641] for more information.

 There are several REST configuration files available by default. They are ready to use. You can also analyze them to see how to write your own REST configuration.

 When using custom sensors on the **Cluster Probe**, please copy your files to every cluster node installation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) ^[181], as well as in [alarms](#) ^[219], [logs](#) ^[228], [notifications](#) ^[3216], [reports](#) ^[3252], [maps](#) ^[3276], [libraries](#) ^[3235], and [tickets](#) ^[230].

Parent Tags Shows [Tags](#) ^[139] that this sensor [inherits](#) ^[140] from its [parent device, group, and probe](#) ^[133]. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

REST SPECIFIC

Timeout (Sec.)	<p>Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).</p>
Request Method	<p>Choose an HTTP request method to determine how the sensor will request the REST API.</p> <ul style="list-style-type: none">▪ GET (default): Use the GET method to request the REST API.▪ POST: Use the POST method to request the REST API.
Postdata	<p>This field is only visible when you select the POST Request Method setting above. Enter the data part for the POST request here.</p>
Request Protocol	<p>Define the security of the HTTP request. Choose between:</p> <ul style="list-style-type: none">▪ HTTP (default): Send the REST query via insecure HTTP.▪ HTTPS: Send the REST query via secure HTTPS.
Authentication Method	<p>Select the authentication method for access to the REST API. Choose between:</p>

REST SPECIFIC

- **No authentication (default):** Do not use any authentication for the request.
- **Basic authentication:** Use simple username and password authentication.
- **Basic authentication with Windows credentials from parent device:** Use the Windows credentials from the parent device. See section [Inheritance of Settings](#)^[137] for more information.
- **Token:** Use a **JSON Web Token (JWT)** or **OAuth2 Bearer Token** for authentication.

User	This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.
Password	This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.
Token	This field is only visible if you enable token authentication above. Enter a JWT or OAuth2 Bearer Token that is required by the REST API for authentication.
HTTP Headers	Define if you want to send custom HTTP headers to the target URL. Choose between: <ul style="list-style-type: none"> ▪ Do not use custom HTTP headers ▪ Use custom HTTP headers
Custom HTTP Headers	<p>This field is only available if you select using custom headers above. Enter a list of custom HTTP headers with their respective values that you want to transmit to the URL you define above, each pair in one line. The syntax of a header-value pair is header1:value1</p> <p> The sensor does not support the header field names user-agent, content-length, host.</p> <p> Ensure the HTTP header statement is valid! Otherwise, the sensor request will not be successful.</p>
REST Query	<p>This field shows the REST query that this sensor executes. To change it, enter a valid query for the target REST API. The syntax is: [:port]/path[?var1=val1&...]</p> <p> The first part of the address is always inherited from the parent device's address. Only enter the path to the REST endpoint of the parent device. You can override the port if necessary.</p>

REST SPECIFIC

For example, if you add the sensor to a probe device, a query to the REST API of your PRTG installation that returns the number of sensors on the probe would look like this:

```
/api/table.json?id=1&passhash=<passhash>&username=<username>&c
```

REST Configuration

Shows the REST configuration file that the sensor uses to map returned JSON or XML into sensor values. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

HTTP Proxy Settings	<p>The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.</p> <ul style="list-style-type: none"> ⓘ This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see System Administration—Core & Probes^[3368]. ⓘ The SSL Certificate Sensor^[2635] and the SSL Security Check Sensor^[2646] do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.
Name	<p>Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.</p>

PROXY SETTINGS FOR HTTP SENSORS

Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	<p>If the proxy requires authentication, enter the username for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>
Password	<p>If the proxy requires authentication, enter the password for the proxy login.</p> <p> Only basic authentication is available! Please enter a string or leave the field empty.</p>

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations.
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Define Sensor Channels and Select Channel Values

In your REST configuration file, you have to define which values of the returned JSON or XML will be mapped to which sensor channels.

- A sensor channel is defined by the channel key in your REST configuration. See the **JSON Return Format: Minimum Example** in section [Custom Sensors](#)³⁶⁴¹.
- A channel value is defined by an expression that retrieves and processes the value from the JSON source. The expression can contain [JSONPath](#)¹⁶⁶⁰, [gval operators](#)¹⁶⁶¹, and [functions](#)¹⁶⁶⁶.

Example

For this example, we take PRTG as REST endpoint and query the sensor status statistics for the local probe. The REST query that we enter in the sensor settings looks like this:

```
/api/table.json?id=1&passhash=<passhash>&username=<username>&content=sensorxref&
noraw=1&filter_basetype=probe&columns=totalsens=extraw,upsens=extraw
downsens=extraw,partialdownsens=extraw,warnsens=extraw,pausedsens=extraw,
unusualsens=extraw,undefinedsens=extraw,downacksens=extraw
```

This REST query will return some JSON, for example:

```
{
  "prtg-version": "17.3.33.2517",
  "treesize": 1,
  "state": "ok",
  "sensorxref": [
    {
      "totalsens": 28,
      "upsens": 18,
      "downsens": 0,
      "partialdownsens": 0,
      "warnsens": 0,
      "pausedsens": 9,
      "unusualsens": 1,
      "undefinedsens": 0,
      "downacksens": 0
    }
  ]
}
```

Your REST configuration has to translate this JSON for the sensor. It has to be available as JSON template (*template) in the `\Custom Sensors\rest` sub-directory of your PRTG probe system. See section [Custom Sensors](#) ³⁶⁴¹ for details about the JSON return format.

The following example returns two channels from the JSON resource that will be added to the sensor in PRTG, **Total** (total sensor count) and **Alarms** (sensors in error status), each selected by their keys in the returned JSON.

```
{
  "prtg": {
    "result": [
      {
        "channel": "Total" ,
        "value": $.sensorxref[0].totalsens
      },
      {
        "channel": "Alarms" ,
        "value": $.sensorxref[0].downsens
      }
    ]
  }
}
```

 There are several REST configuration files available in the `\Custom Sensors\rest` folder by default. They are ready to use. You can also analyze them to see how to write your own REST configuration.

JSONPath

The REST Custom sensor uses **JSONPath** to assign values from the returned JSON to sensor channels. With JSONPath you provide the path to the value in the JSON source that you want to monitor in a sensor channel.

 The JSONPath implementation that PRTG uses for the REST Custom sensor might differ from other JSONPath implementations. You can [test and debug your definitions](#)¹⁶⁶⁸ using the command line. To test simple JSONPath expressions and calculations, you can also use [JSONPath Online Evaluator](#)¹⁶⁷⁰, for example. Please note that this tool might not work properly with complex JSONPath expressions that PRTG supports.

Example

To demonstrate the practical usage of JSONPath, we use this JSON example that a REST query might have returned as reference in this section.

```
{
  "devices": [
    {
      "firmware": {
        "id": "0.7",
        "date": "2017-05-18T17:11:43.7049944Z",
        "channel": "beta"
      },
      "networks": {
        "a": {
          "rx_bytes": 35985021,
          "tx_bytes": 7229493,
          "rx_errors": 0,
          "rx_dropped": 476,
          "tx_bytes": 7229493,
          "tx_packets": 35518,
          "tx_errors": 0,
          "tx_dropped": 1
        },
        "b": {
          "rx_bytes": 40085321,
          "tx_bytes": 55294975
        }
      }
    },
    {
      "networks": {
        "a": {
          "rx_bytes": 63685865,
          "tx_bytes": 7229472
        }
      }
    }
  ]
}
```

REST CUSTOM SENSOR: JSONPATH

Root The dollar sign (\$) matches the root element of the JSON data.

Child You can match a child with `.<key>` or `[<key>]`

- `.<key>` must only contain letters, numbers, and underscore (_). Hyphens (-) are not supported.
- `[<key>]` must only contain a number or a quoted string.

Example

This expression matches **35985021** in the example above:

```
$.devices.0.networks.a.rx_bytes
```

You get the same result with this expression:

```
["$devices"][0]["networks"]["a"]["rx_bytes"]
```

If an element contains a hyphen (-), the `.<key>` notation does not work. Use the `[<key>]` notation in this case:

```
["$data"][0]["system-stats"]["temps"]["Board (CPU)"]
```

Wildcard To match multiple values, you can use the asterisk symbol (*).

- `.*`
- `[*]`

Example

This expression matches **35985021** and **40085321** in the example above:

```
$.devices[0].networks.*.rx_bytes
```

Recursive Descent You can match all sub-items of a node with two dots (..).

Example

This expression matches **7229493** and **55294975** and **7229472** in the example above:

```
$...tx_bytes
```

Union You can match multiple children with `[<key 1>,<key 2>,<...>]`.

Example

This expression matches **35985021** and **7229493** in the example above:

```
$.devices.0.networks.a["rx_bytes","tx_bytes"]
```

REST CUSTOM SENSOR: JSONPATH

- Slice** You can match multiple children of an array with [**<begin>:<end>**] or [**<begin>:<end>:<step>**].
- By default, **begin**, **end**, and **step** are either integers or empty.
 - The default approach is to go step by step from the first array element to the last element.
 - **Step** can also be a negative integer to go through the array in reversed order.

Example

This expression matches **63685865** in the example above:

```
$.devices[-1:].networks.a.rx_bytes
```

- Current** The @ symbol matches the current element.

Example

This expression matches to **40.085321** and **55.294975** in the example above and can be used to receive a percentage value:

```
$.devices[1].networks.a.["rx_bytes","tx_bytes"](@/100000000*100)
```

- Filter** You can filter matches with [**?<expression>**].

Example

This expression matches **35985021** in the example above because the first device is the only one with a beta channel:

```
$.devices[?@.firmware.channel=="beta"].networks.a.rx_bytes
```

- Script** You can modify matches with (**<expression>**) and keys with [**<expression>**].

Example

This expression matches **true** and **false** in the example above because only the first device has a beta channel:

```
$.devices[*](@.firmware.channel=="beta")
```

- Placeholder** Placeholders give access to values of wildcards in a match. A placeholder **#n** (where **n** is a natural number) represents the value of the **n**th wildcard. You can use this in the keys of JSON arrays.

Example

REST CUSTOM SENSOR: JSONPATH

This expression creates a JSON map from **ids** to the corresponding firmware channel and matches **{"0.7":"beta"}** in the example above:

```
{$.devices[#0].id:$.devices[*].channel}
```

 This is an extension of the official JSONPath.

- Constant
 - Numeric constants as 64-bit floating point: **12345.678**
 - String constants with double quotes: **"switch"**
 - Boolean constants: **true** and **false**

- Operator
 - Parentheses control the order of evaluation: **(<expression>)**
 - Arrays with square brackets: **[<expression>, <expression>, ...]**
 - Objects: **{<expression>:<expression>, <expression>:<expression>, ...}**
 - Conditionals: **<condition> ? <expression> : <expression>**

Calculating Channel Values and Functions

You can perform calculations with the values of the source JSON or XML. The sensor uses the Paessler **gval** package for the calculations. Please refer to the [gval documentation](#)¹⁶⁷⁰ for details.

The following operators and functions are available to calculate channel values.

REST CUSTOM SENSOR: OPERATORS

	Oper ator	Description	Operand Type	Out put Type
Infix Modifiers	+	plus	number	number
	-	minus	number	number
	*	times	number	number
	**	power of	number	number
	%	modulo	number	number

REST CUSTOM SENSOR: OPERATORS

	/	divide	number	number
	&	bitwise and	number	number
		bitwise or	number	number
	^	bitwise xor	number	number
	<<	shift left	number	number
	>>	shift right	number	number
Logical Infix Operators	>	greater than	number/string	bool
	>=	equal or greater than	number/string	bool
	<	less than	number/string	bool
	<=	equal or less than	number/string	bool
	==	equal	any	bool
	!=	not equal	any	bool
	=~	match regular expression	string	bool
	!~	mismatch regular expression	string	bool
	in	contains element	any, array	bool
	&&	and	and	bool
	or	or	bool	
??	coalescence	any	any	

REST CUSTOM SENSOR: OPERATORS

Prefix Operators	-	negative	number	number
	~	bitwise not	number	number
	!	not	bool	bool

REST CUSTOM SENSOR: FUNCTIONS

duration
(start,end)

- Calculates the nanoseconds between start and end.
- Both parameters must be RFC3339 date time strings.

Example

```
duration($.devices[0].firmware.date, "017-05-18T17:11:43.7049944Z")
```

now()

- Returns the current date time in RFC3339.

Example

```
duration($.devices[0].firmware.date, now())
```

number(string,
[base])

- Converts a string to a floating point number.
- If the base is not set, it will be detected via the prefix of the string.
 - "0": base = 8
 - "0X": base = 16
 - otherwise: base = 10
- Decimals are only supported at base 10.

Examples

```
number("10.5")
number("a", 16)
```

len(object/
array/string)

- Returns the length of an array or string and counts the number of properties in a JSON object.

Example

```
len($..(number(@)))
```

REST CUSTOM SENSOR: FUNCTIONS

This expression counts every number or string that can be converted into a number. It returns **13** in the example above.

sum(array-/
object-of-
numbers)

- Returns the sum over an array of numbers.

Example

```
sum([1,2,3])
```

This expression returns **6**.

mean(array-/
object-of-
numbers)

- Returns the average value of an array of numbers.

Example

```
mean([1,2,3])
```

This expression returns **2**.

lookup(string,
string, string, ...)

- Returns the index of the given string in a string list, or **-1** if the string is not found.

Example

```
lookup($.device[0].firmware.channel, "stable", "beta", "alpha")
```

This expression returns **1** because **\$.device[0].firmware.channel** resolves to **beta**.

implode(array-/
object-of-string,
string)

- Returns the concatenation of each string in the array, separated by the given string.

Example

```
implode($.tx_bytes, ",")
```

This expression returns **7229493,7229472**.

Generic Channels

You can create a template in your REST configuration that defines generic channels. Generic channels are created based on the data that the REST endpoint returns. When the returned value is an array or object, the sensor will create a channel for each element and concatenate the corresponding key to the channel name.

Example

Imagine you want to have a total byte channel for each network card that is defined in the JSON example above. You can do this by creating a dynamic channel like in the following example.

```
{
  "prtg": {
    "result": [
      {
        "value": {
          "Total bytes on device" + #0 + " in network " + #1: $.devices.*.networks[*](@.rx_bytes + @.tx_by
        },
        "CustomUnit": "Bytes"
      }
    ]
  }
}
```

 Every channel must have unique name. Channels cannot be removed once they are added and will keep their last received value. New channels can be added.

XML Sources

If the REST source returns XML instead of JSON, the sensor will transform the XML result to JSON before replacing the value paths with source values. Because of this, you will not know the structure of the source JSON to correctly provide the paths.

In this case, manually execute the sensor executable **rest.exe** from the **\Sensor System** subfolder of the PRTG probe system. Execute **rest.exe** with the address of the XML endpoint and the parameter **passthrough**. The rest executable will return the converted XML to JSON result that you can use to define the desired paths..

```
rest.exe <xml-endpoint-url> passthrough
```

Usage and Debugging

To create a suitable REST configuration for the sensor, you might want to check the returned JSON or XML and see what happens when your mapping rules apply.

The REST Custom sensor is an EXE sensor, so you can test and debug your configuration by executing **rest.exe** with several parameters. The **rest.exe** is located in the **\Sensor System** subfolder of the PRTG program directory.

Command syntax:

```
rest.exe url template|passthrough|channelDiscovery [flags]
```

REST.EXE: PARAMETERS

url	<ul style="list-style-type: none">▪ Address of the REST API endpoint that returns JSON or XML
template	<ul style="list-style-type: none">▪ Fully qualified path and file name of your REST configuration file used to map the JSON result to the sensor
passthrough	<ul style="list-style-type: none">▪ No mapping, only returning the queried JSON or XML▪ Useful to analyze XML that has been converted to JSON
channelDiscovery	<ul style="list-style-type: none">▪ Creates a channel for every number or boolean in the returned JSON or XML▪ If possible, it converts string values to number or boolean values.

REST.EXE: FLAGS

-authtoken <string>	<ul style="list-style-type: none">▪ JWT or OAuth2 Bearer Token to send with the request in authorization header as Bearer
-authusername <string>	<ul style="list-style-type: none">▪ User name for basic authentication
-authuserpwd <string>	<ul style="list-style-type: none">▪ User password for basic authentication
-post <string>	<ul style="list-style-type: none">▪ {1 0}▪ Default: 0▪ 0 results in a GET request.▪ 1 results in a POST request.
-proxy <string>	<ul style="list-style-type: none">▪ Proxy server connection
-proxyusername <string>	<ul style="list-style-type: none">▪ Proxy user name with basic authentication
-proxyuserpwd <string>	<ul style="list-style-type: none">▪ Proxy user password with basic authentication
-tlsignore <string>	<ul style="list-style-type: none">▪ {1 0}▪ Default: 0

REST.EXE: FLAGS

- 1 will accept self-signed certificates on HTTPS connections
- customheaders <string> ▪ key1:val1|key2:val2|...
- template ▪ Returns the discovered template is you use **channelDiscovery**.
- timeout <integer> ▪ Sensor timeout in seconds
▪ Default: 10

More

Paessler JSONPath

- <https://github.com/PaesslerAG/jsonpath>

Paessler gval

- <https://github.com/PaesslerAG/gval>

JSONPath Online Evaluator

- <http://jsonpath.com/>

Knowledge Base: Can I create a sensor to monitor the number of paused or unknown sensors?

- <https://kb.paessler.com/en/topic/2653>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.110 REST Dell EMC Capacity Sensor

The REST Dell EMC Capacity sensor monitors the disk usage on a Dell EMC storage system via the REST Application Programming Interface (API). Dell EMC systems that provide a REST API are EMC Unity Family, EMC Unity All Flash, EMC Unity Hybrid, and EMC UnityVSA.

The sensor shows the following:

- Response time
- Total size
- Free size
- Free space in percent
- Used size in percent
- Subscribed size
- Compression in percent

✓ Sensor REST Dell EMC Capacity ★★★★☆
OK

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Free Space

59 % 0 % 100 %

<p>Compression</p> <p>0 %</p>	<p>Free Size</p> <p>48,049,946,624...</p>	<p>Response Time</p> <p>2,779 msec</p>
<p>Subscribed Size</p> <p>66,571,993,088...</p>	<p>Total Size</p> <p>80,262,201,344...</p>	<p>Used Size</p> <p>32212254720 %</p>

Channel	ID	Last Value	Minimum	Maximum	
Compression	5	0 %	0 %	0 %	⚙️
Downtime	-4				⚙️
Free Size	2	48,049,9...	48,049,946,624 Byte	48,049,946,624 Byte	⚙️
Free Space	3	59 %	59 %	59 %	⚙️
Response Time	0	2,779 m...	1,065 msec	14,244 msec	⚙️
Subscribed Size	6	66,571,9...	66,571,993,088 Byte	66,571,993,088 Byte	⚙️
Total Size	1	80,262,2...	80,262,201,344 Byte	80,262,201,344 Byte	⚙️
Used Size	4	3221225...	32212254720 %	32212254720 %	⚙️

REST Dell EMC Capacity Sensor

Sensor in Other Languages

Dutch: **REST Dell EMC Capacity**, French: **Capacité de l'EMC REST Dell**, German: **REST Dell EMC Capacity**, Japanese: **REST Dell EMC ? ?**, Portuguese: **REST Dell EMC Capacidade**, Russian: **Емкость REST Dell EMC**, Simplified Chinese: **REST Dell EMC ? ?**, Spanish: **Capacidad de Dell EMC con REST**

Remarks

- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

REST SPECIFIC SETTINGS

Authentication Method Select the authentication method for access to the REST API. Choose between:

- **Basic authentication:** Use simple username and password authentication.
- **Basic authentication with Windows credentials from parent device (default):** Use the Windows credentials from the parent device. See section [Inheritance of Settings](#)^[137] for more information.

User This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.

Password This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.

Certificate Acceptance Select the kind of certificates that you want the sensor to accept for the connection. Choose between:

- **Accept trusted certificates only (default):** Accept only trusted certificates issued by a Certificate Authority (CA).
- **Accept all certificates:** Accept all certificates, including self-signed certificates.

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

PROXY SETTINGS FOR HTTP SENSORS

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

-  Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
-  To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

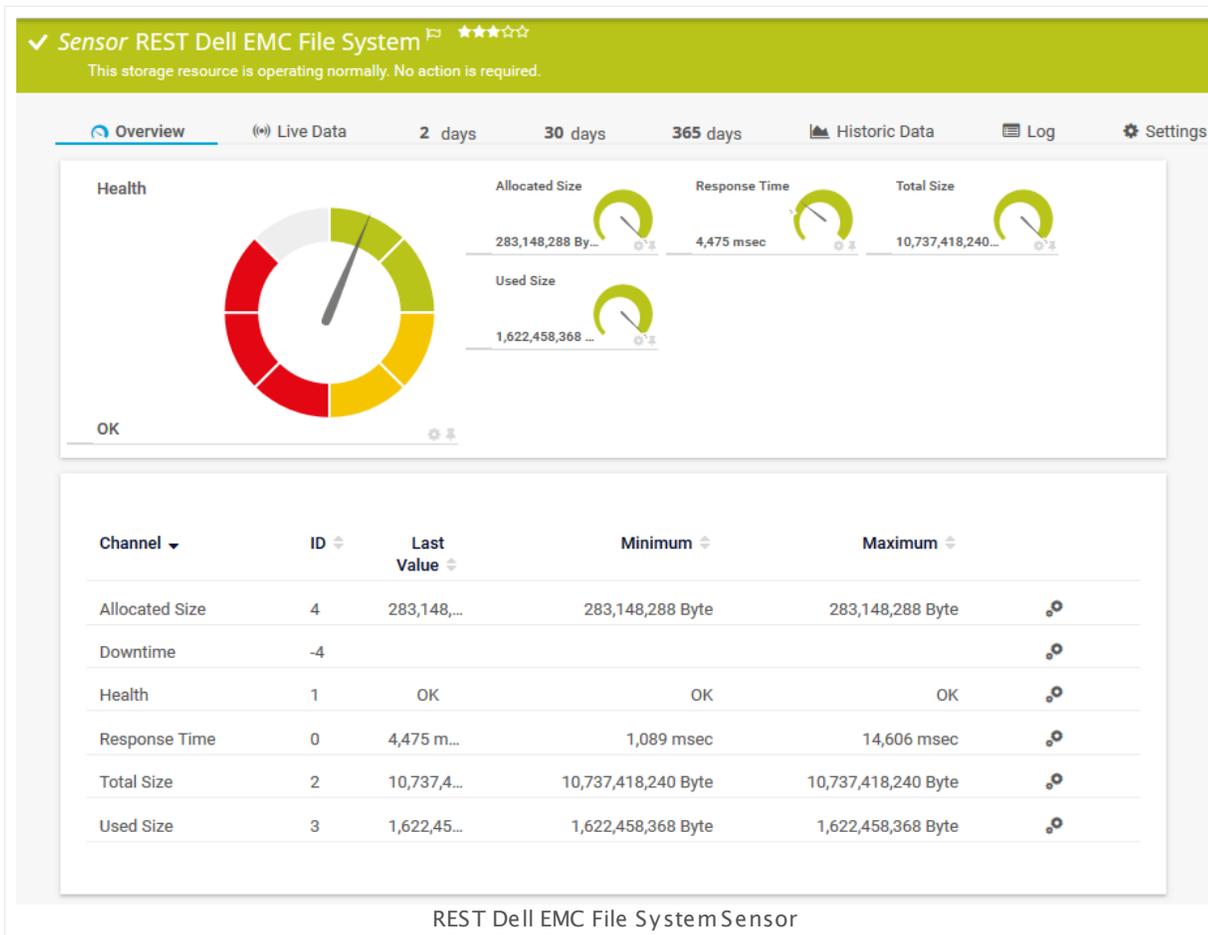
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.111 REST Dell EMC File System Sensor

The REST Dell EMC File System sensor monitors the health of a file system on a Dell EMC storage system via the REST Application Programming Interface (API). Dell EMC systems that provide a REST API are EMC Unity Family, EMC Unity All Flash, EMC Unity Hybrid, and EMC UnityVSA.

The sensor shows the following:

- Response time
- Health status
 - Up [status](#)¹⁹⁵: OK, OK But Minor Warning
 - **Warning** status: Degraded, Minor Issue
 - **Down** status: Major Issue, Critical Issue, Non Recoverable
- Total size
- Used size
- Allocated size



Sensor in Other Languages

Dutch: **REST Dell EMC bestandssysteem**, French: **Système de fichiers EMC REST Dell**, German: **REST Dell EMC Dateisystem**, Japanese: **REST Dell EMC ? ? ? ? ? ? ?**, Portuguese: **REST Dell EMC Sistema de arquivos**, Russian: **Файловая система REST Dell EMC**, Simplified Chinese: **REST Dell EMC ? ? ? ?**, Spanish: **Sistema de archivos de Dell EMC con REST**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the file systems you want to monitor. PRTG will create one sensor for each file system you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

EMC SPECIFIC

EMC File System	Select the file system(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-----------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMC SPECIFIC

EMC File System	Shows the name of the file system that the sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!
-----------------	---

REST SPECIFIC SETTINGS

Authentication Method	Select the authentication method for access to the REST API. Choose between: <ul style="list-style-type: none">▪ Basic authentication: Use simple username and password authentication.▪ Basic authentication with Windows credentials from parent device (default): Use the Windows credentials from the parent device. See section Inheritance of Settings^[137] for more information.
User	This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.
Password	This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.
Certificate Acceptance	Select the kind of certificates that you want the sensor to accept for the connection. Choose between: <ul style="list-style-type: none">▪ Accept trusted certificates only (default): Accept only trusted certificates issued by a Certificate Authority (CA).▪ Accept all certificates: Accept all certificates, including self-signed certificates.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	---

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.112 REST Dell EMC LUN Sensor

The REST Dell EMC LUN sensor monitors a logical unit number (LUN) on a Dell EMC storage system via the REST Application Programming Interface (API). Dell EMC systems that provide a REST API are EMC Unity Family, EMC Unity All Flash, EMC Unity Hybrid, and EMC UnityVSA.

The sensor shows the following:

- Health status
 - **Up** [status](#)¹⁹⁵: OK, OK But Minor Warning
 - **Warning** status: Degraded, Minor Issue
 - **Down** status: Major Issue, Critical Issue, Non Recoverable
- Total size
- Compression in percent
- Allocated size
- Metadata size
- Allocated metadata size
- Snapshot size
- Allocated snapshot size



Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the LUNs you want to monitor. PRTG will create one sensor for each LUN that you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

EMC SPECIFIC

EMC LUN Select the file LUN(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMC SPECIFIC

EMC LUN Shows the name of the LUN that the sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

REST SPECIFIC SETTINGS

Authentication Method Select the authentication method for access to the REST API. Choose between:

- **Basic authentication:** Use simple username and password authentication.
- **Basic authentication with Windows credentials from parent device (default):** Use the Windows credentials from the parent device. See section [Inheritance of Settings](#)^[137] for more information.

User This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.

Password This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.

REST SPECIFIC SETTINGS

- Certificate Acceptance** Select the kind of certificates that you want the sensor to accept for the connection. Choose between:
- **Accept trusted certificates only (default):** Accept only trusted certificates issued by a Certificate Authority (CA).
 - **Accept all certificates:** Accept all certificates, including self-signed certificates.
- Timeout (Sec.)** Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings

The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

PROXY SETTINGS FOR HTTP SENSORS

Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login.  Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.  Only basic authentication is available! Please enter a string or leave the field empty.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ³³¹¹ .  Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between: <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

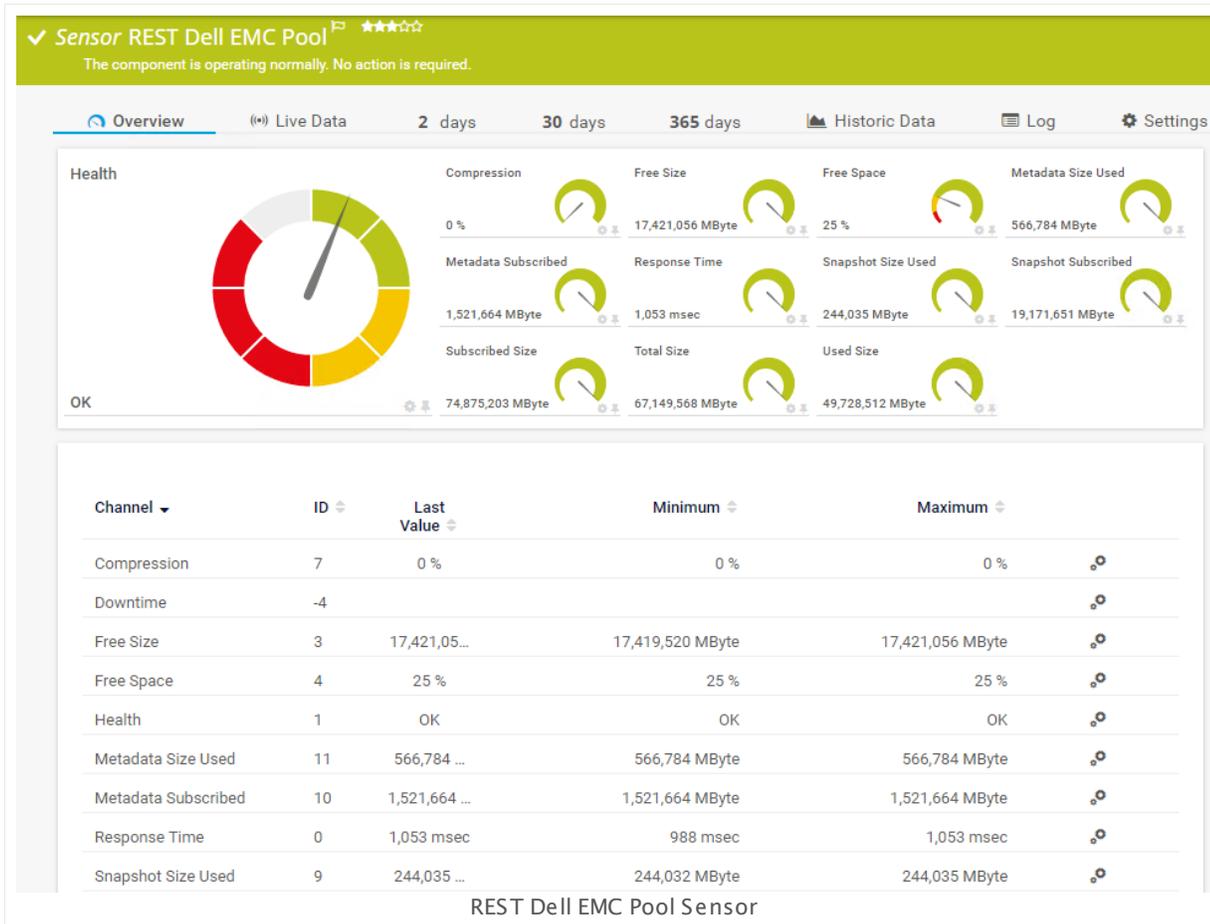
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.113 REST Dell EMC Pool Sensor

The REST Dell EMC Pool sensor monitors a storage pool on a Dell EMC storage system via the REST Application Programming Interface (API). Dell EMC systems that provide a REST API are EMC Unity Family, EMC Unity All Flash, EMC Unity Hybrid, and EMC UnityVSA.

The sensor shows the following:

- Response time
- Health status
 - **Up** [status](#)¹⁹⁵: OK, OK But Minor Warning
 - **Warning** status: Degraded, Minor Issue
 - **Down** status: Major Issue, Critical Issue, Non Recoverable
- Total, free, used, and subscribed size
- Free space in percent
- Compression in percent
- Snapshot subscribed and snapshot size used
- Metadata subscribed and metadata size used



Sensor in Other Languages

Dutch: REST Dell EMC Pool, French: Pool EMC REST Dell, German: REST Dell EMC Pool, Japanese: REST Dell EMC ? ? ? , Portuguese: REST Dell EMC Pool, Russian: Пул REST Dell EMC, Simplified Chinese: REST Dell EMC ? , Spanish: Grupo de Dell EMC con REST

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will perform a meta scan before you actually add this sensor type and requires basic information for this scan in advance. Provide the requested information in the appearing window. During the scan, PRTG will recognize all items available for monitoring based on your input. The following settings differ in comparison to the sensor's settings page.

Select the storage pools you want to monitor. PRTG will create one sensor for each pool that you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

EMC SPECIFIC

EMC Pool

Select the file pool(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags

Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMC SPECIFIC

- EMC Pool** Shows the name of the pool that the sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

REST SPECIFIC SETTINGS

- Authentication Method** Select the authentication method for access to the REST API. Choose between:
- **Basic authentication:** Use simple username and password authentication.
 - **Basic authentication with Windows credentials from parent device (default):** Use the Windows credentials from the parent device. See section [Inheritance of Settings](#)^[137] for more information.

REST SPECIFIC SETTINGS

User	This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.
Password	This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.
Certificate Acceptance	Select the kind of certificates that you want the sensor to accept for the connection. Choose between: <ul style="list-style-type: none"> ▪ Accept trusted certificates only (default): Accept only trusted certificates issued by a Certificate Authority (CA). ▪ Accept all certificates: Accept all certificates, including self-signed certificates.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> ▪  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

HTTP Proxy Settings	<p>The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.</p>
---------------------	--

PROXY SETTINGS FOR HTTP SENSORS

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#)³³⁶⁸.
-  The [SSL Certificate Sensor](#)²⁶³⁵ and the [SSL Security Check Sensor](#)²⁶⁴⁶ do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name	Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.
Port	Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.
User	If the proxy requires authentication, enter the username for the proxy login.
	 Only basic authentication is available! Please enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.
	 Only basic authentication is available! Please enter a string or leave the field empty.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

-  Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings ³³¹¹ .
	 Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p> To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

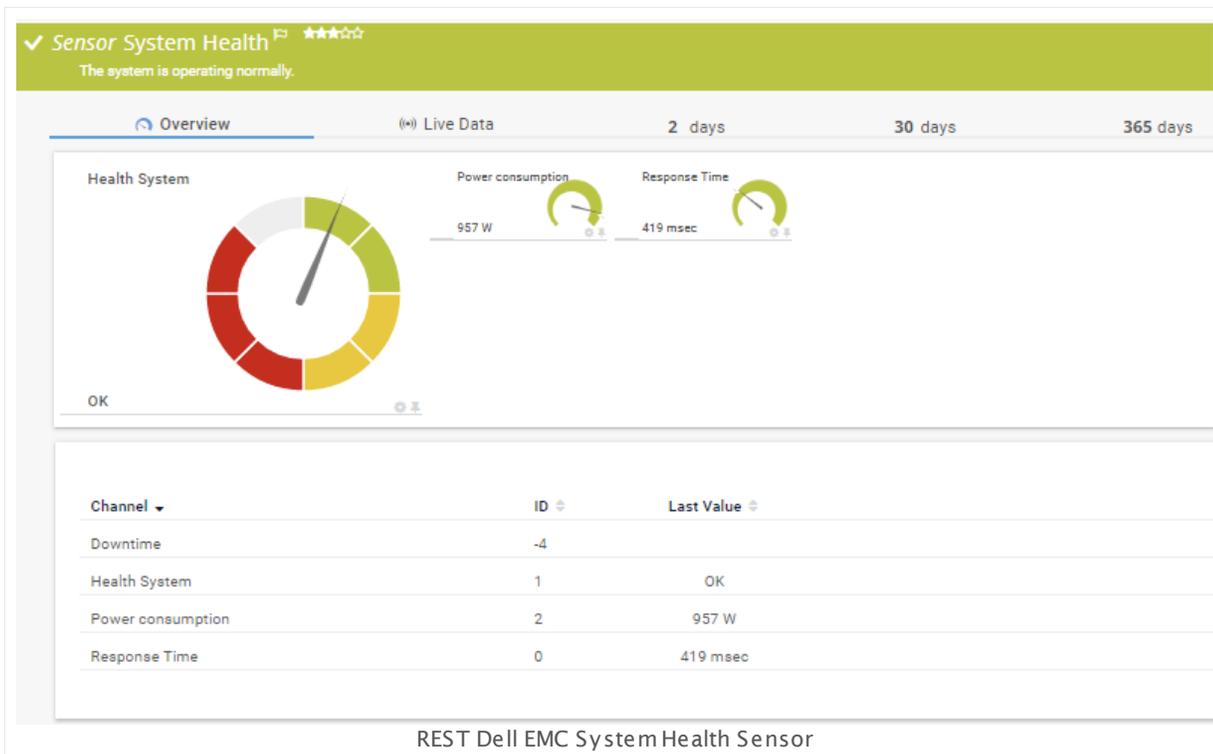
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.114 REST Dell EMC System Health Sensor

The REST Dell EMC System Health sensor monitors the health status of a Dell EMC storage system via the REST Application Programming Interface (API). Dell EMC systems that provide a REST API are EMC Unity Family, EMC Unity All Flash, EMC Unity Hybrid, and EMC UnityVSA.

The sensor shows the following:

- Health status
 - **Up status** ¹⁹⁵¹: OK, OK But Minor Warning
 - **Warning status**: Degraded, Minor Issue
 - **Down status**: Major Issue, Critical Issue, Non Recoverable
- Power consumption



Sensor in Other Languages

Dutch: **REST Dell EMC systeem gezondheid**, French: **État du système EMC REST Dell**, German: **REST Dell EMC Systemzustand**, Japanese: **REST Dell EMC ? ? ? ? ? ? ?**, Portuguese: **REST Dell EMC Funcionamento do sistema**, Russian: **Работоспособность системы REST Dell EMC**, Simplified Chinese: **REST Dell EMC ? ? ? ? ? ? ?**, Spanish: **Estado del sistema de Dell EMC con REST**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

BETA

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

REST SPECIFIC SETTINGS

Authentication Method Select the authentication method for access to the REST API. Choose between:

- **Basic authentication:** Use simple username and password authentication.
- **Basic authentication with Windows credentials from parent device (default):** Use the Windows credentials from the parent device. See section [Inheritance of Settings](#)^[137] for more information.

User This field is only visible if you enable basic authentication above. Enter a username for the REST API. Please enter a string.

Password This field is only visible if you enable basic authentication above. Enter a password for the REST API. Please enter a string.

Certificate Acceptance Select the kind of certificates that you want the sensor to accept for the connection. Choose between:

- **Accept trusted certificates only (default):** Accept only trusted certificates issued by a Certificate Authority (CA).
- **Accept all certificates:** Accept all certificates, including self-signed certificates.

Timeout (Sec.) Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is **900** seconds (15 minutes).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

PROXY SETTINGS FOR HTTP SENSORS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

HTTP Proxy Settings The proxy settings determine how a sensor connects to a given URL. You can enter data for an HTTP proxy server that sensors will use when connecting via HTTP or HTTPS.

-  This setting affects monitoring only and determines the behavior of HTTP sensors. To change proxy settings for the core server, see [System Administration—Core & Probes](#).
-  The [SSL Certificate Sensor](#) and the [SSL Security Check Sensor](#) do not support HTTP proxies, but you can configure connections via SOCKS proxies in their sensor settings.

Name Enter the IP address or DNS name of the proxy server to use. If you leave this field empty, no proxy will be used.

Port Enter the port number of the proxy. Often, port 8080 is used. Please enter an integer value.

User If the proxy requires authentication, enter the username for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

Password If the proxy requires authentication, enter the password for the proxy login.

-  Only basic authentication is available! Please enter a string or leave the field empty.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.115 Sensor Factory Sensor

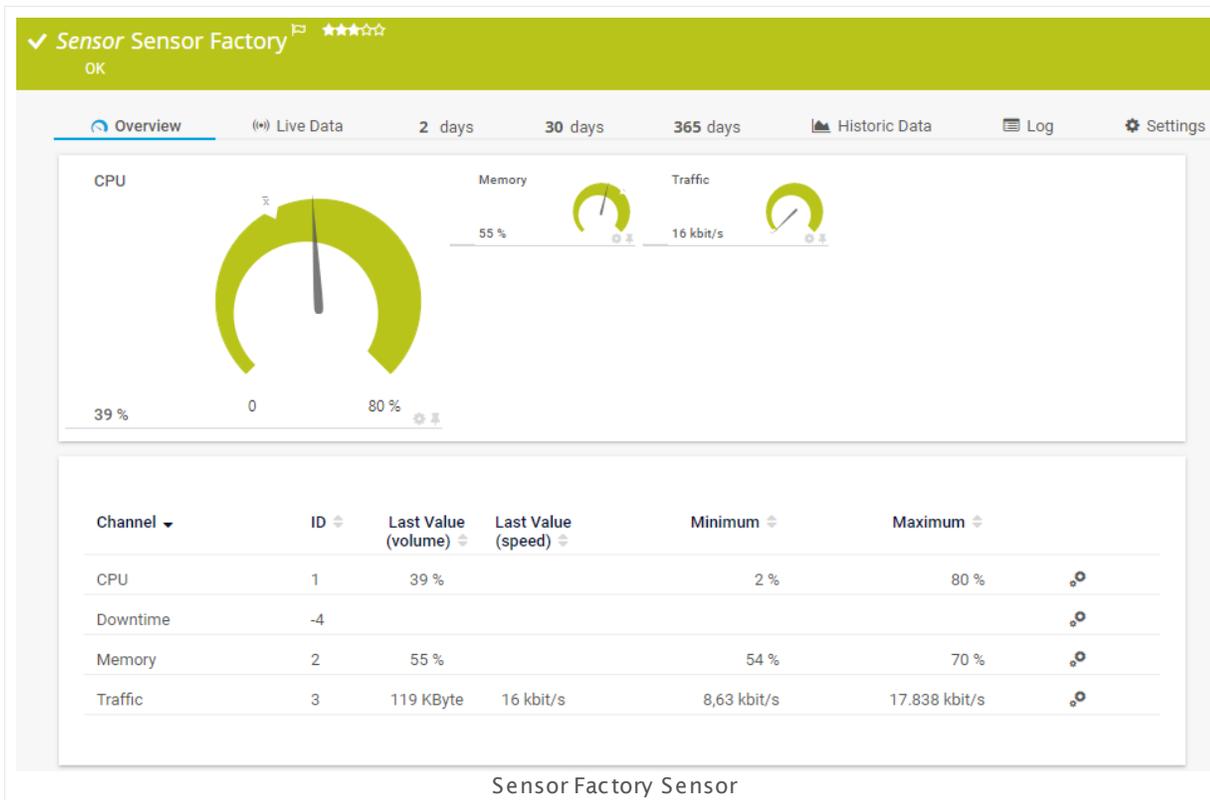
The Sensor Factory sensor is a powerful tool that allows you to monitor entire business processes that involve several components.

You can define one or more channels that combine monitoring results from other sensors or devices. You can create your own individual sensor with channels based on data from other sensors or devices.

Samples for usage are:

- Show single channels of one or more sensors in one graph.
 - Use the data from single channels of one or more sensors to calculate new values (for example, you can subtract, multiply, and divide).
 - Create graphs with data from other sensor channels and add horizontal lines at specific vertical positions.
- ❗ The Sensor Factory sensor does not show values in the **Downtime** channel because they cannot be calculated for this sensor type.
- ❗ If you want to create only a cumulated sensor status based on specific source sensors, we recommend that you use the [Business Process Sensor](#) instead.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **Sensor Fabriek**, French: **Capteur combiné**, German: **Formelsensor**, Japanese: ? ? ? ? ? ? ? ? , Portuguese: **Sensor de fórmula**, Russian: **Фабрика сенсоров**, Simplified Chinese: ? ? ? ? ? ? , Spanish: **Sensor Factory**

Remarks

- This sensor [does not support more than 50 channels](#)^[1721] officially.
- Ensure the [scanning interval](#)^[1725] of this sensor is equal to or greater than the scanning interval of the source sensor(s) to avoid incorrect sensor behavior. For example, "no data" messages or erratic changes of the sensor status can be a result of an invalid scanning interval.
- Knowledge Base: [How can I monitor the overall status of the business process "Email"?](#)
- The Sensor Factory sensor might not work with [flow sensors](#)^[3514]. Sensor types using **active flow timeout**, this is, [NetFlow and jFlow sensors](#)^[430], are not supported by the Sensor Factory sensor.
- [Reports](#)^[204] cannot show uptime or downtime data for this sensor type.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type per PRTG installation.

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR FACTORY SPECIFIC SETTINGS

Channel Definition	<p>Enter a channel definition for the sensor. Using a specific syntax, you can refer to data from channels of other sensors here. You can also calculate values. Enter one channel definition for each new channel you want to add to this sensor.</p> <p> For more information, see section Define Sensor Channels^[1729] below.</p>
--------------------	--

SENSOR FACTORY SPECIFIC SETTINGS

Error Handling

Define the behavior of the sensor if one of the sensors defined above is in an error status. In this case, you can set the sensor factory sensor either to down or to warning status. Choose between:

- **Factory sensor shows error status when one or more source sensors are in error status:** If at least one sensor that you use in a channel definition is in a **Down** status, the Factory sensor shows a **Down** status as well until all referred sensors leave this status. While the Sensor Factory sensor is **Down**, it will still show data of all available sensor channels.
 - ❗ If a [lookup definition](#)³⁶⁹³ or an [error limit](#)³¹⁶² triggers the error status of the source sensor, the Sensor Factory will not show a **Down** status. This is because the Sensor Factory should only show this status if it cannot calculate values.
- **Factory sensor shows warning status when one or more source sensors are in error status:** If at least one sensor that you use in a channel definition is in a **Down** status, the factory sensor shows a **Warning** status until all referred sensors leave the **Down** status.
 - ❗ If a [lookup definition](#)³⁶⁹³ or an [error limit](#)³¹⁶² triggers the error status of the source sensor, the Sensor Factory will not show a **Warning** status. This is because the Sensor Factory should only show this status if it cannot calculate values.
- **Use custom formula:** Define the status of the Factory sensor by adding a status definition in the field below.

SENSOR FACTORY SPECIFIC SETTINGS

Status Definition

This field is only visible if you choose **Use custom formula** above. Define when the sensor will switch to a **Down** status. You can use the `status()` function in combination with Boolean operations. For advanced users it is also possible to calculate a status value.

 For more information, see section [Define Sensor Status](#)¹⁷³⁶ below.

If a Sensor Has No Data

Choose how this Sensor Factory sensor reacts if a sensor referred to in the channel definition does not provide any data (for example, because it is paused or does not exist). Choose between:

- **Do not calculate factory channels that use the sensor:** For defined channels that use one or more sensor(s) that deliver no data, no data is shown.
- **Calculate the factory channels and use zero as source value:** If a sensor that you use in a channel definition does not deliver any data, zero values will be filled in instead. The sensor factory calculates the channel value and shows it using these zero values.

 If a sensor in the channel of a factory sensor has no data, the factory sensor will always show a **Warning** `status`¹⁹⁵, no matter which of the above options you select.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Define Sensor Channels

The channels of a Sensor Factory sensor are controlled by the **Channel Definition** text field. Using a special syntax you can refer to other sensor channels, calculate values, and add horizontal lines. You can define factory sensor channels using data from any other sensor's channels on your PRTG server.

Example

You see a definition of two factory sensor channels. Both use the `channel()` function, which simply collects data from the channels of other sensors in your monitoring and displays them:

```
#1:Local Probe Health
channel(1001,0)
#2:Local Traffic Out[kbit]
channel(1004,1)
```

The first channel of the factory sensor (**#1**) collects data from the **Health** channel (**ID 0**) of the **Probe Health** sensor (**ID 1001**) running on the Local Probe device. The second channel (**#2**) collects data from the **Traffic out** channel (**ID 1**) of a traffic sensor (**ID 1004**) measuring the system's local network card. Both channels will be shown together in the factory sensor's data tables and graphs.

The basic syntax for a sensor factory channel definition looks like this:

```
#<id>:<name>[<unit>]
<formula>
```

For each channel one section is used. A section begins with the **#** sign. Function names in formulas are not case sensitive.

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number that is greater than 0.
- **<name>** is the name of the factory sensor's channel (displayed in graphs and tables).
- **[<unit>]** is an optional unit description for the factory sensor's channel (for example, bytes). If you do not provide a unit, the sensor factory selects a suitable unit string automatically (recommended).
- **<formula>** contains the formula to calculate the factory sensor's channel. For the formula, you can use the following functions: [channel\(\)](#)¹⁷³¹, [min\(\)](#)¹⁷³², [max\(\)](#)¹⁷³², [avg\(\)](#)¹⁷³², or [percent\(\)](#)¹⁷³³.

Define Sensor Channels—Formula Calculations

Within a formula, the following elements are allowed to perform calculations with the values that are returned by one or more functions.

- Basic operations: + (add), - (subtract), * (multiply), / (divide)
Example: $3 + 5 * 2$
- Brackets: ()
Example: $3 * (2 + 6)$

- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
If the comparison resolves to true, the value is **10,000**; if false, the value is **0**. For delta sensors the speed is compared.

Example

You see a Sensor Factory channel definition with calculation.

```
#1:Traffic Total x Minus Traffic Out y
( channel(2001,-1) - channel(1004,1) ) * 2
```

This full channel definition results in a factory sensor that shows a calculation with values from two channels (channel IDs **-1** and **1**) of two traffic sensors (sensor IDs **2001** and **1004**). The returned values are subtracted and then multiplied by two.

Channels can be gauge values (for example, ping ms) or delta values (for example, traffic kbit/s). Not all combinations are allowed in a formula.

- ⓘ When performing percentage calculation, please use the [percent\(\) Function](#)¹⁷³⁰ to make sure you obtain the expected values!

There are calculations you **cannot** do:

- You cannot add/subtract a delta from a gauge channel (and vice-versa).
- You cannot multiply two delta channels.
- You cannot compare a delta with a gauge channel.
- You cannot use a channel of (another) Sensor Factory sensor channel in the formula.

Define Sensor Channels—channel() Function

The **channel()** function allows to read the data from a channel of a different sensor. The syntax is:

```
channel(<sensorId>,<channelId>)
```

The parameters are:

- **<sensorId>** is the ID of the sensor. It is displayed on the sensor details page in the [page header bar](#)¹⁸⁵.
- **<channelId>** is the ID of the sensor channel. It is displayed in the respective field of the [channel settings](#)³¹⁶².

Example

```
channel(2001,2)
```

This function reads the data from channel ID **2** of the sensor with the ID **2001**.

```
#1:Sample  
channel(2001,2)
```

This full channel definition reads the data from channel ID **2** of the sensor with the ID **2001** and displays it in the first factory sensor channel (**#1**), without any additional calculations.

Define Sensor Channels—min() and max() Functions

The **min()** and **max()** functions return the minimum or maximum of two values. The syntax is:

```
min(<a>,<b>)  
max(<a>,<b>)
```

Values for **<a>** and **** are either numbers or [channel\(\)](#) functions.

Examples

```
min(10,5)
```

This function in the first line returns **5**, because this is the smaller value out of 10 and 5.

```
min( channel(2001,1),channel(2002,1) )
```

This function returns the minimum of the values of channel **1** of the sensor with ID **2001** and channel **1** of the sensor with ID **2002**.

Define Sensor Channels—avg() Function

The **avg()** function returns the average of the two values. This equals: $(a+b) / 2$. The syntax is:

```
avg(<a>,<b>)
```

Values for **<a>** and **** are either numbers or [channel\(\)](#) functions.

Examples

```
avg(20,10)
```

This function returns **15**: $(20+10) / 2 = 15$.

```
avg( channel(2001,1),channel(2002,1) )
```

This function returns the average of channel **1** of the sensor with ID **2001** and channel **1** of the sensor with ID **2002**.

Define Sensor Channels—percent() Function

The **percent()** function calculates the percent value of two given values, for example, a channel and a fixed value. The syntax is:

```
percent(<source>,<maximum>[,<unit>])
```

The parameters are:

- **<source>** is the value the percent is calculated for. This is usually a [channel\(\)](#)¹⁷³¹ function.
- **<maximum>** is the limit value used for the percent calculation.
- **[<unit>]** is an optional unit the maximum is provided in. You can use constants with this function (see [Constants](#)¹⁷³⁵ section below for a list). This can be used for absolute values (for example, [Ping sensors](#)¹⁵²⁹) or calculated delta values (for example, traffic sensors). If no unit is provided, **1** will be used.
 - ❗ The sensor adds the unit string **%** automatically.

PRTG will calculate: $\text{<source>} / \text{<maximum>} * \text{<unit>} * 100$

Examples

```
#1:Usage Traffic In
percent(channel(2001,0),100,kilobit)
#2:Usage Traffic Out
percent(channel(2001,1),100,kilobit)
```

This full channel definition results in a factory sensor that shows two channels of a traffic sensor (sensor ID **2001**): Traffic in (channel ID **0**) and traffic out (channel ID **1**). The sensor displays the values % of maximum bandwidth (100 kilobit/second).

```
#1:Ping %
percent(channel(2002,0),200)
```

This full channel definition results in a factory sensor that shows the **Ping Time** channel (channel ID **0**) of a Ping sensor (sensor ID **2002**). The sensor displays the values as a percentage of 200 ms.

Define Sensor Channels—Horizontal Lines

You can add lines to the graph using a formula without **channel()** function. Use a fixed value instead. The syntax is:

```
#<id>:<name>[<unit>]
<value>
```

The parameters are:

- **<id>** is the ID of the factory sensor's channel and must be a unique number greater than 1. Although the sensor does not show a horizontal line as a channel, the ID has to be unique.
- **<name>** is the name of the factory sensor's channel. PRTG does not display this name in graphs and tables, but you can use it as a comment to describe the nature of the line.
- **[<unit>]** is an optional unit description (for example, kbit/s). If you do not provide a unit, PRTG applies the line automatically to the scale of the first factory sensor channel. If your factory sensor uses different units, provide a unit to make sure the line is added for the right scale. Enter the unit exactly as shown in your graph's legend. If you enter a unit that does not yet exist in your graph, a new scale will be added automatically.
- **<value>** contains a number defining where the line will be shown in the graph.

Examples

```
#5:Line at 100ms [ms]
100
```

This channel definition results in a graph that shows a horizontal line at the value of **100** on the **ms** scale.

```
#6:Line at 2 Mbit/s [kbit/s]
2000
```

This channel definition results in a graph that shows a horizontal line at the value of **2000** on the **kbit/s** scale.

```
#1:Ping Time
channel(2002,0)
#2:Line at 120ms [ms]
120
```

This full channel definition results in a factory sensor that shows the **Ping Time** channel (channel ID **0**) of a Ping sensor (sensor ID **2002**). Additionally, the sensor graphs will show a horizontal line at **120 ms**.

Define Sensor Channels—Constants

The following constants are defined and can be used in calculations:

- **one** = 1
- **kilo** = 1000
- **mega** = 1000 * kilo
- **giga** = 1000 * mega
- **tera** = 1000 * giga
- **byte** = 1
- **kilobyte** = 1024
- **megabyte** = 1024 * kilobyte
- **gigabyte** = 1024 * megabyte
- **terabyte** = 1024 * gigabyte
- **bit** = 1/8
- **kilobit** = kilo / 8
- **megabit** = mega / 8

- **gigabit** = giga / 8
- **terabit** = tera / 8

Define Sensor Status—status() Function

You can control the status of a Sensor Factory sensor via the **Status Definition** text field if you enable the custom formula option in the [Sensor Settings](#)¹⁷²¹. Using a special syntax, you can define when the factory sensor changes to a **Down** status. In all other cases, the sensor will be in an **Up** status. The syntax is:

```
status(sensorID) <boolean> status(sensorID)
```

The parameters are:

- **<sensorid>** is the ID of the sensor you want to check the status of. It is displayed on the sensor details page in the [page header bar](#)¹⁸⁵.
- **<boolean>** is one of the Boolean operators **AND**, **OR**, or **NOT**. If the resulting expression is **true**, the factory sensor will change to a **Down** status.

Examples

```
status(2031) AND status(2044)
```

This changes the factory sensor to a **Down** status if both sensors, with IDs **2031** and **2044**, are **Down**. Otherwise the factory sensor shows an **Up** status.

```
status(2031) OR status(2044)
```

This changes the factory sensor to a **Down** status if at least one of the sensors with ID **2031** or ID **2044** is **Down**. Otherwise the factory sensor shows an **Up** status.

```
status(2031) AND NOT status(2044)
```

This changes the factory sensor to a **Down** status if the sensor with ID **2031** is **Down**, but the sensor with ID **2044** is **not** in a **Down** status. Otherwise the factory sensor shows an **Up** status.

! A `status()` function with **NOT** has to be connected with **AND** or **OR** if it is combined with other `status()` functions:

```
status(sensorID) AND NOT status(sensorID)
status(sensorID) OR NOT status(sensorID)
```

```
( status(2031) AND status(2044) ) OR status(2051)
```

This changes the factory sensor to a **Down** status if both the sensor with ID **2031** and the sensor with ID **2044** is **Down**, or if the sensor with ID **2051** is **Down**. Otherwise the factory sensor shows an **Up** status.

Additionally, the following elements are allowed to perform calculations and comparisons with the values that are returned by the status functions:

- Basic operations: + (add), - (subtract), * (multiply), / (divide)
Example: $3 + 5 * 2$
- Brackets: ()
Example: $3 * (2 + 6)$
- Compare: = (equal), <> (not equal), > (greater), < (less), >= (greater or equal), <= (less or equal)
If the comparison resolves to true, the value is **10,000**; if false, the value is **0**. For delta sensors the speed is compared.

Internally, the `status()` function returns the downtime channel of the sensor in hundreds of percent (10,000 = 100%).

- **true** corresponds to a value of 10,000, which is a **Down** status.

- **false** corresponds to a value of 0, which is an **Up** status.

If you understand this, you are able to use more complex formulas.

Example

```
( status(1031) + status(1032) + status(1033) + status(1034) ) >= 20000
```

This changes the factory sensor to a **Down** status if at least any two of the sensors with IDs **1031**, **1032**, **1033**, or **1034** are **Down**. Otherwise the factory sensor shows an **Up** status.

i You can also use the `status()` function in [channel definitions](#)¹⁷²⁹. Using this functionality, it is possible, for example, to display the numeric status value of sensors in a factory sensor channel.

Using Factory Sensors in a Cluster Setup

If you run PRTG in [Clustering](#)¹³⁰ mode, please note these additional facts:

- If you add a Sensor Factory sensor underneath the **Cluster Probe**, and in the Sensor Factory formula you refer to a channel of a sensor running on the **Cluster Probe** as well, the Sensor Factory sensor will show the data of all cluster nodes for this sensor channel.
- If you add a Sensor Factory sensor underneath the **Local Probe**, and in the Sensor Factory formula you refer to a channel of a sensor running on the **Cluster Probe**, the Sensor Factory sensor will only show data of the primary master node for this sensor channel.

More

Video Tutorial: How to Create a Factory Sensor for the Monitoring of Complex Processes in PRTG

- <https://www.paessler.com/support/videos/prtg-advanced/factory-sensor>

Knowledge Base: How can I monitor the overall status of the business process "Email"?

- <https://kb.paessler.com/en/topic/60737>

Knowledge Base: What can I do with PRTG's Sensor Factory Sensors?

- <https://kb.paessler.com/en/topic/583>

Paessler Blog: Monitoring Business Processes—Transformation of Technical Outages to the Real Business Impact

- <https://www.paessler.com/blog/2014/06/26/all-about-prtg/monitoring-business-processes>

Edit Sensor Channels

To change display settings and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel.

 For detailed information, see the [Sensor Channels Settings](#)^[3160].

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

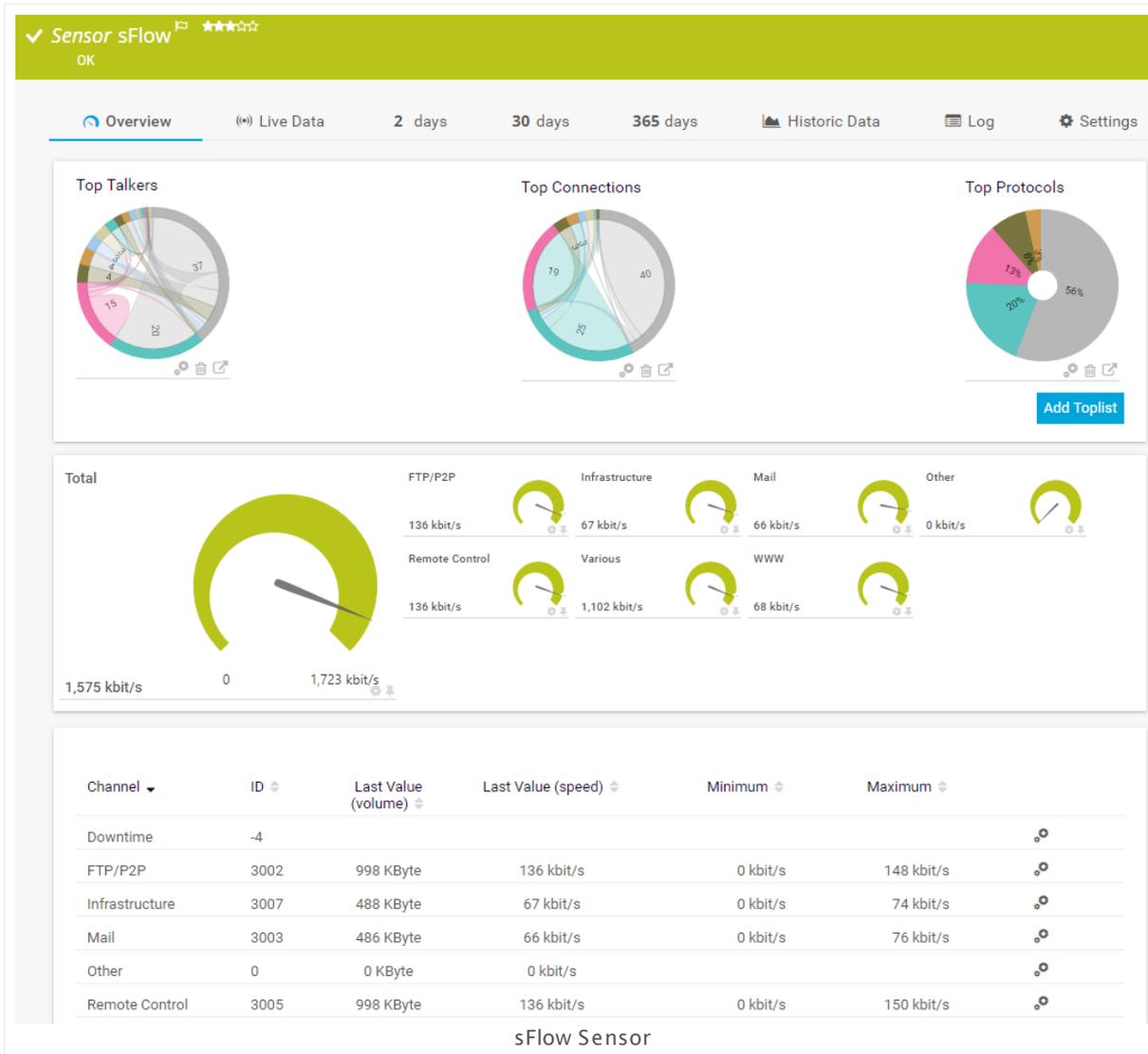
7.8.116 sFlow Sensor

The sFlow sensor receives traffic data from an sFlow V5 compatible device and shows the traffic by type. Only header traffic will be analyzed. Ensure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

This sensor can show the following traffic types in kbit per second:

- Chat (IRC, AIM)
- Citrix
- FTP/P2P (file transfer)
- Infrastructure (network services: DHCP, DNS, Ident, ICMP, SNMP)
- Mail (mail traffic: IMAP, POP3, SMTP)
- NetBIOS
- Remote control (RDP, SSH, Telnet, VNC)
- WWW (web traffic: HTTP, HTTPS)
- Total traffic
- Other protocols (other UDP and TCP traffic)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- You must enable sFlow V5 export on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
- The sensor accepts RAW data only. The stream must be sent via IPv4.
- This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
- There are several [limitations](#) for this sensor type.
- Paessler Website: [Paessler sFlow Tester](#)
- Knowledge Base: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)
- Knowledge Base: [Where is the volume line in graphs?](#)

- For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" and "Extended flow" formats are supported. "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

 We recommend that you use the sFlow tester for debugging. Please download it here: [Paessler sFlow Tester](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on UDP Port	Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is 6343 . Please enter an integer value.  When configuring export, ensure you select the appropriate sFlow version 5.
Sender IP	Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on IP Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device.

 When configuring export, ensure you select the appropriate sFlow version 5.

Log Stream Data to Disk (for Debugging) Define if you want the probe to write a logfile of the stream and packet data to the data folder (see [Data Storage](#)³⁷³⁴). Choose between:

- **None (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **Only for the 'Other' channel:** Only write logfiles of data that is not filtered otherwise and therefore accounted to the default **Other** channel.
- **All stream data:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

CHANNEL CONFIGURATION

Channel Selection Define the categories the sensor accounts the traffic to. There are different groups of traffic available. Choose between:

- **Web:** Internet web traffic.
- **File Transfer:** Traffic caused by FTP.
- **Mail:** Internet mail traffic.
- **Chat:** Traffic caused by chat and instant messaging.
- **Remote Control:** Traffic caused by remote control applications, such as RDP, SSH, Telnet, and VNC.
- **Infrastructure:** Traffic caused by network services, such as DHCP, DNS, Ident, ICMP, and SNMP.
- **NetBIOS:** Traffic caused by NetBIOS communication.
- **Citrix:** Traffic caused by Citrix applications.

CHANNEL CONFIGURATION

- **Other Protocols:** Traffic caused by various other protocols via UDP and TCP.

For each traffic group, you can select how many channels will be used for each group, that is, how detailed the sensor divides the traffic. For each group, choose between:

- **No (X icon):** Do not account traffic of this group in its own channel. All traffic of this group is accounted to the default channel named **Other**.
- **Yes (check mark icon):** Count all traffic of this group and summarize it into one channel.
- **Detail (magnifier icon):** Count all traffic of this group and further divide it into different channels. The traffic appears in several channels as shown in the **Content** column.
 - ⚠ Extensive use of this option can cause load problems on your probe system. We recommend setting specific, well-chosen filters for the data you really want to analyze.

 You can change the default configuration for groups and channels. For details, see this Knowledge Base article: [How can I change the default groups and channels for xFlow and Packet Sniffer sensors?](#)

FILTERING

Include Filter Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.

 For detailed information, see section [Filter Rules](#)¹⁷⁵¹ below.

Exclude Filter First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.

 For detailed information, see section [Filter Rules](#)¹⁷⁵¹ below.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

PRIMARY TOPLIST

Primary Toplist	<p>Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:</p> <ul style="list-style-type: none">▪ Top Talkers▪ Top Connections▪ Top Protocols▪ [Any custom toplists you have added]
-----------------	--

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)  for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#) .

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats )
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats )
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats )
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to sFlow sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address

More

Paessler Website: Paessler sFlow Tester

- <https://www.paessler.com/tools/sflowtester>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Related Topics

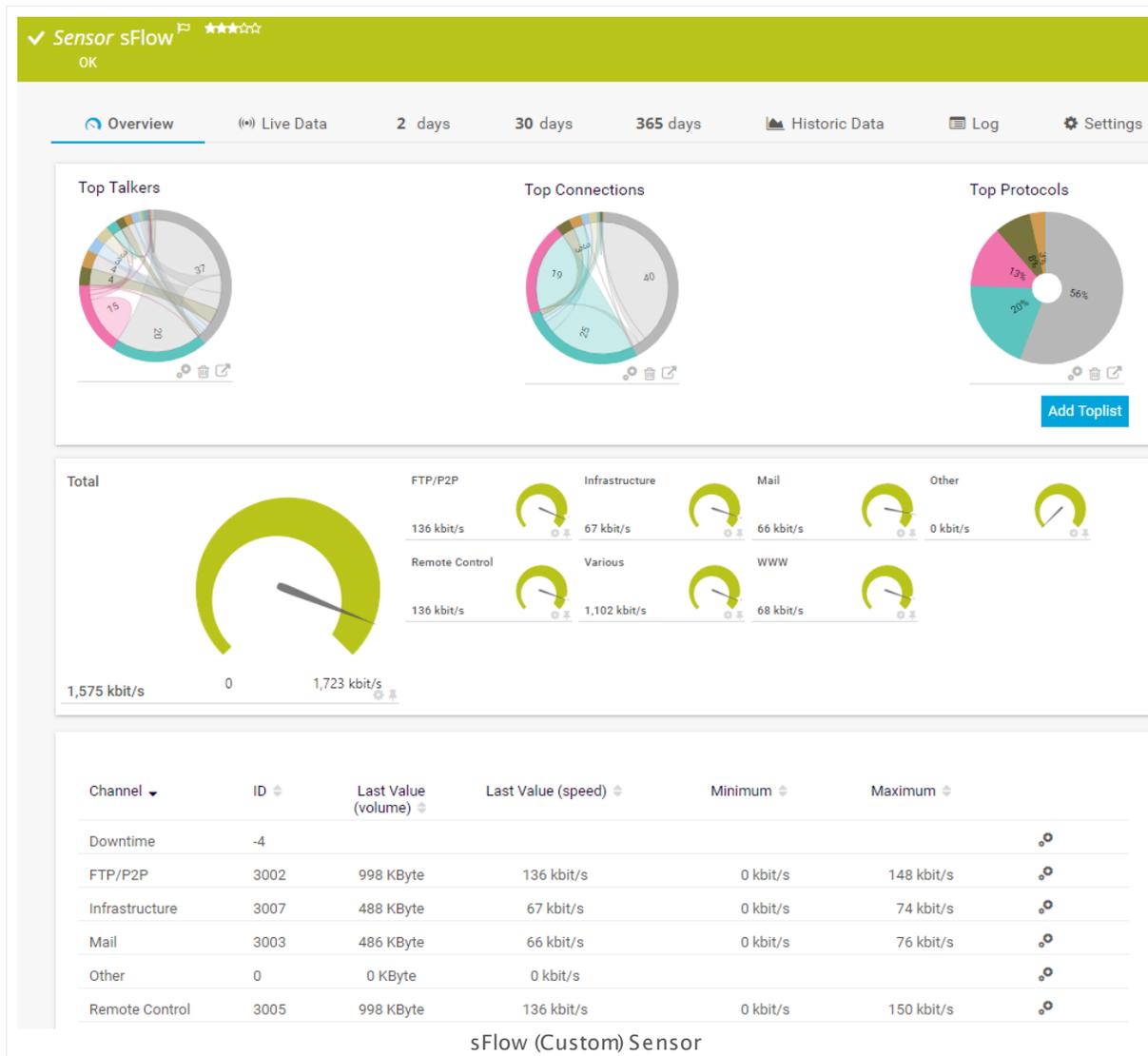
- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.117 sFlow (Custom) Sensor

The sFlow (Custom) sensor receives traffic data from an sFlow V5 compatible device and shows the traffic by type. Please make sure the device matches the sFlow version V5! There are several filter options available to divide traffic into different channels.

- This sensor can show traffic by type individually according to your needs.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: sFlow (Custom), French: sFlow (personnalisé), German: sFlow (Benutzerdef.), Japanese: sFlow(? ? ? ?), Portuguese: sFlow (customizado), Russian: sFlow (нестандартный), Simplified Chinese: sFlow(? ? ?), Spanish: sFlow (Personalizado)

Remarks

- You must enable sFlow V5 export on the monitored device for this sensor to work. The device must send the flow data stream to the IP address of the PRTG probe system on which the sensor is set up (either a local or remote probe).
 - The sensor accepts RAW data.
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - There are several [limitations](#)¹⁷⁵⁵ for this sensor type.
 - Paessler Website: [Paessler sFlow Tester](#)
 - Knowledge Base: [Where is the volume line in graphs?](#)
 - For a general introduction to the technology behind flow monitoring, please see manual section [Monitoring Bandwidth via Flows](#)³⁵¹⁴.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Limitations of This Sensor Type

There are some limitations that you want to consider before using this sensor type:

- Only sFlow version 5 datagrams are supported
- Only IPv4 flows are supported
- Only the "raw packet header" format is supported
- Only the "Flow sample" and "Extended flow" formats are supported. "Counter" formats cannot be processed
- PRTG processes only samples where the source ID matches the ifIndex of the input interface (avoiding double counted traffic) and ascending sequence numbers.
- Sample packets have to be of ethernet type "IP" (with optional VLAN tag)
- Sampled packets of type TCP and UDP are supported

 We recommend that you use the sFlow tester for debugging. Please download it here: [Paessler sFlow Tester](#)

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SFLOW SPECIFIC SETTINGS

Receive sFlow Packets on UDP Port	<p>Enter the UDP port number on which the flow packets are received. It must match the one you have configured in the sFlow export options of your hardware router device. Default value is 6343. Please enter an integer value.</p> <p> When configuring export, ensure you select the appropriate sFlow version 5.</p>
Sender IP	<p>Enter the IP address of the sending device you want to receive the sFlow from. Enter an IP address to receive data from a specific device only, or leave the field empty to receive data from any device on the specified port.</p>
Receive sFlow Packets on IP	<p>Select the IP address(es) on which PRTG listens to sFlow packets. The list of IP addresses shown here is specific to your setup. To select an IP address, add a check mark in front of the respective line. The IP address selected here must match the one configured in the sFlow export options of your hardware router device.</p> <p> When configuring export, ensure you select the appropriate sFlow version 5.</p>

Channel Definition	<p>Enter a channel definition to divide the traffic into different channels. Write each definition in one line. All traffic for which no channel is defined will be accounted to the default channel named Other.</p> <p> For detailed information, see section Channel Defintions for xFlow and Packet Sniffer Sensors³⁶⁹⁰.</p> <p> Extensive use of many filters can cause load problems on your probe system. We recommend defining specific, well-chosen filters for the data you really want to analyze.</p>
Log Stream Data to Disk (for Debugging)	<p>Define if you want the probe to write a logfile of the stream and packet data to the data folder (see Data Storage³⁷³⁴). Choose between:</p> <ul style="list-style-type: none"> ▪ None (recommended): Do not write additional logfiles. Recommended for normal use cases. ▪ Only for the 'Other' channel: Only write logfiles of data that is not filtered otherwise and therefore accounted to the default Other channel. ▪ All stream data: Write logfiles for all data received. <p> Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.</p>

FILTERING

- Include Filter** Define if you want to filter any traffic. If you leave this field empty, all traffic will be included. To include specific traffic only, define filters using a special syntax.
-  For detailed information, see section [Filter Rules](#)¹⁷⁶⁴ below.
- Exclude Filter** First, the filters defined in the **Include Filter** field are considered. From this subset, you can explicitly exclude traffic, using the same syntax.
-  For detailed information, see section [Filter Rules](#)¹⁷⁶⁴ below.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

PRIMARY TOPLIST

Primary Toplist Define which will be your primary toplist. It will be shown in maps when adding a toplist object. Choose from:

- **Top Talkers**
- **Top Connections**
- **Top Protocols**
- **[Any custom toplist you have added]**

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.

SCANNING INTERVAL

- **Set sensor to "warning" for 2 intervals, then set to "down":**
Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- ❶ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- ❶ If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- ❶ If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

❶ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

❶ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none">▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p> To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Toplists

For all flow and packet sniffer sensors there are **Toplists** available on the **Overview** tab of a sensor's detail page. Using toplist, you can review traffic data of small time periods in great detail.

 For more information, see section [Toplists](#)³¹⁸⁶.

Filter Rules

The following filter rules apply to all xFlow, IPFIX, and Packet Sniffer sensors.

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁹)
DestinationPort	Any number

FIELD	POSSIBLE FILTER VALUES
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

The following filter rules apply to sFlow sensors only.

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address

More

Paessler Website: Paessler sFlow Tester

- <https://www.paessler.com/tools/sflowtester>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

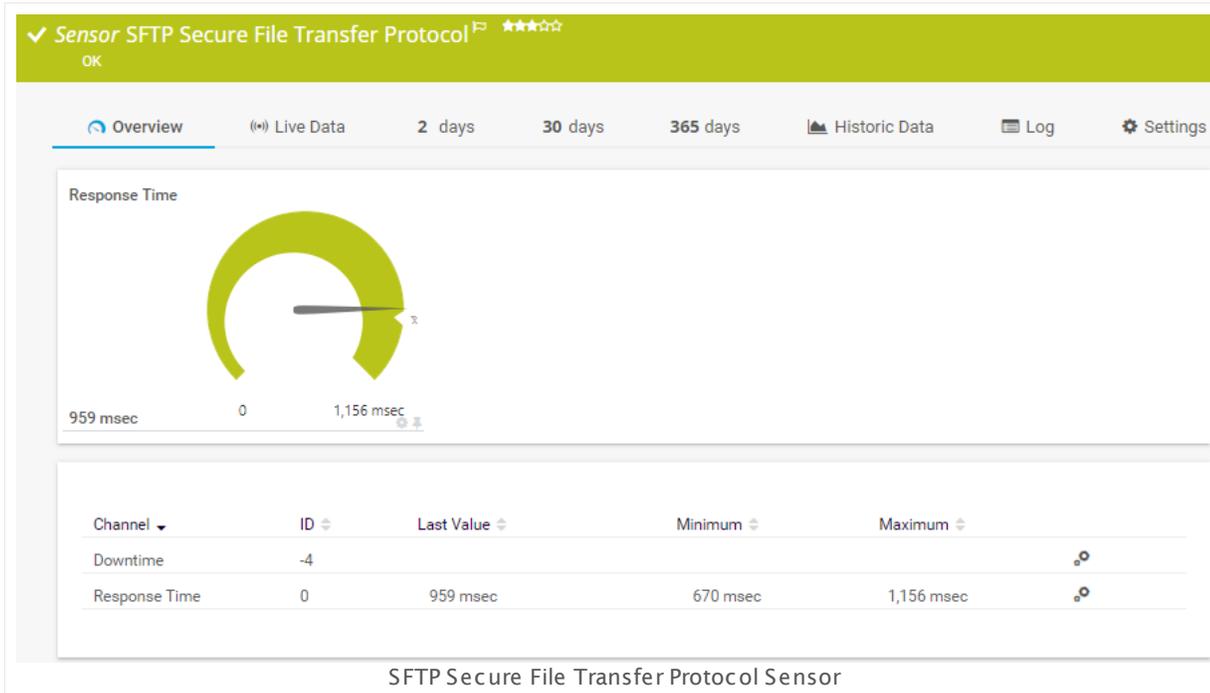
Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁸⁵
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)³⁶⁹⁰

7.8.118 SFTP Secure File Transfer Protocol Sensor

The SFTP Secure File Transfer Protocol sensor monitors FTP servers of a Linux/Unix system using SSH File Transfer Protocol (FTP over SSH).

- It tries to connect to the server and shows the response time.



Sensor in Other Languages

Dutch: **SFTP Secure File Transfer Protocol**, French: **Protocole sécurisé de transfert de fichiers SFTP (Secure File Transfer Protocol)**, German: **SFTP Secure File Transfer Protocol**, Japanese: **SFTP(Secure File Transfer Protocol)**, Portuguese: **SFTP Secure File Transfer Protocol**, Russian: **Защищенный протокол передачи файлов SFTP**, Simplified Chinese: **SFTP ? ? ? ? ? ? ? ?**, Spanish: **SFTP Secure File Transfer Protocol**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.</p>
SSH Port	<p>Define which port this sensor uses for the SSH connection. Choose between:</p> <ul style="list-style-type: none">▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems^[408] section of the device this sensor is created on.▪ Enter custom port number: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	<p>This field is only visible if you choose Enter custom port number above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.</p>
SSH Engine	<p>Select the method you want to use to access data with this SSH sensor^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p>

SSH SPECIFIC

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)¹³³. If you did not change it, this is the recommended default engine.
 - **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
 - **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.
-  The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

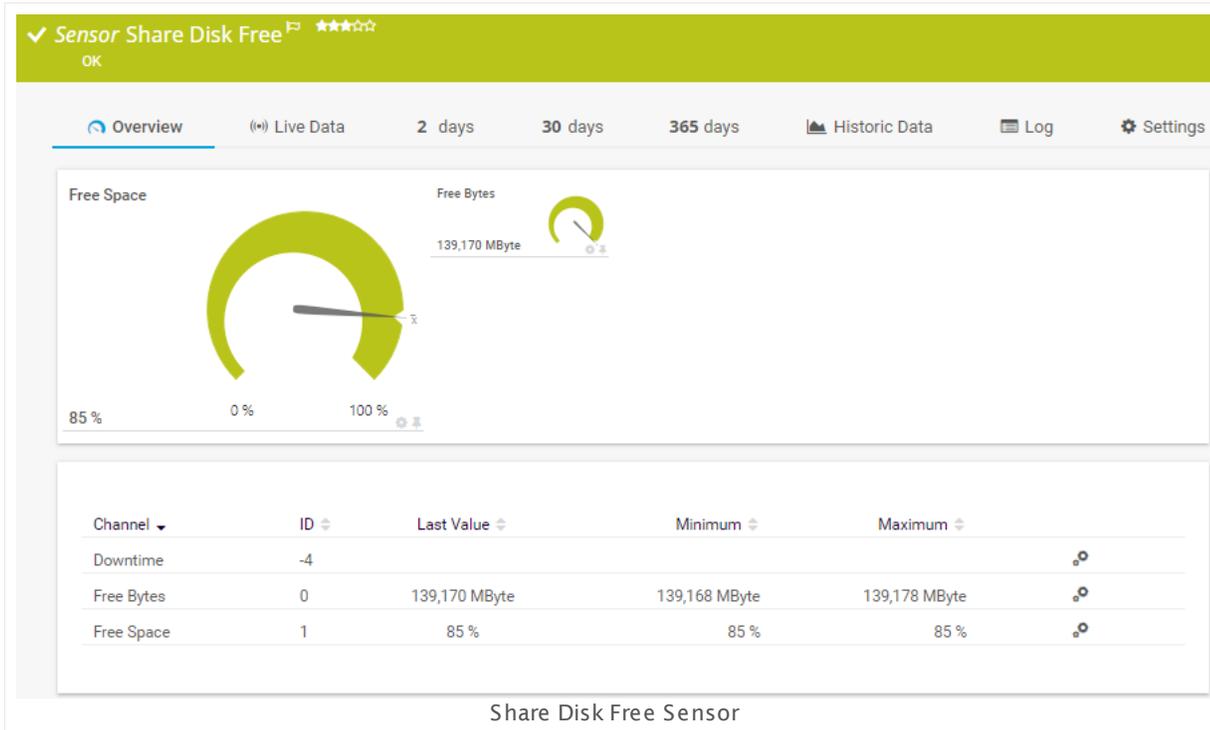
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.119 Share Disk Free Sensor

The Share Disk Free sensor monitors free disk space of a share (Windows/Samba) using Server Message Block (SMB).

- It shows the free disk space in percent and bytes.



Sensor in Other Languages

Dutch: **Share Disk Ruimte**, French: **Espace disque libre partagé**, German: **Freigaben-Speicherplatz**, Japanese: **?** **?** **?** **?** **?** **?** **?** **?** **?** **?**, Portuguese: **Disco livre para compartilhamento**, Russian: **Свободное дисковое пространство общего ресурса**, Simplified Chinese: **?** **?** **?** **?** **?** **?** **?** **?** **?** **?**, Spanish: **Disco libre share**

Remarks

- [Requires](#) ¹⁷⁷⁸ the LanmanServer Windows service to be running on the target device.
- This sensor only works if no quotas are enabled on the target share. If there are quotas enabled for the user account this sensor uses to connect to the share, the absolute value will be okay, but the percentage variable will show wrong values.
- Knowledge Base: [What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: LanmanServer Windows Service

- ✘ To monitor shares on Windows machines, please make sure the **LanmanServer** "Server" Windows service is running on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ℹ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SHARE CONFIGURATION

Share Enter the name of the share this sensor will monitor. Only a share name is allowed here (for example, enter C\$). Please do not enter a complete UNC name here. The server name (\\server) is taken from the parent device of this sensor.

 To provide any shares under Windows, the LanmanServer "Server" Windows service must be running on the target computer.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What can I do if PRTG doesn't succeed with monitoring a share? PE029 PE032

- <https://kb.paessler.com/en/topic/513>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

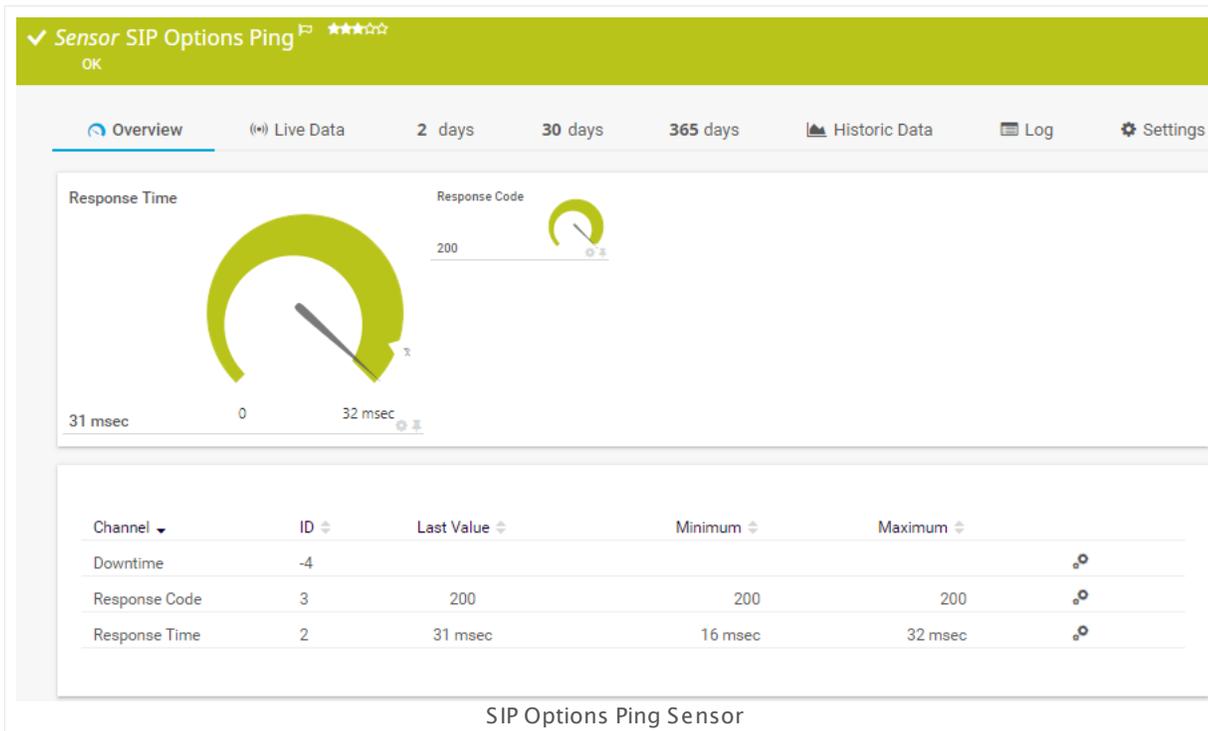
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.120 SIP Options Ping Sensor

The SIP Options Ping sensor monitors the connectivity for a Session Initiation Protocol (SIP) server using SIP options "Ping". You can use it to monitor Voice over IP (VoIP) services. The sensor sends **auth** and **options** requests to the SIP server. It can alert in case of an error.

It can show the following:

- Response time of the SIP server
- Response code: You can individually define the status for each individual response code by editing the [lookup](#) file `prtg.standardlookups.sip.statuscode`



Sensor in Other Languages

Dutch: **SIP Opties Ping**, French: **Ping SIP Options**, German: **SIP Options Ping**, Japanese: **SIP Ping**, Portuguese: **SIP Options Ping**, Russian: **Ping параметров SIP**, Simplified Chinese: **SIP Ping**, Spanish: **Opciones Ping SIP**

Remarks

- [Requires](#) .NET 4.5 or later on the probe system.
- An SIP server might return the error **480 Service temporarily unavailable** until at least one reachable SIP client is connected to the server.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SIP SPECIFIC

Port	<p>Enter the number of the port to which this sensor connects. Please enter an integer value. The default UDP port is 5060.</p>
Username	<p>Enter the username of the SIP account this sensor will log on to after a connection to the SIP server has been established. Please enter a string.</p>
Password	<p>Enter the password of the SIP account this sensor will log on to after a connection to the SIP server has been established. Please enter a string.</p>
Timeout (Sec.)	<p>Enter the timeout for the connection to the SIP server. Please enter an integer value. The maximum value is 300.</p>
Retry Count	<p>If the connection to the SIP server fails, the sensor tries to connect again. Enter the maximum number of retries. After reaching the maximum count, the sensor will show a red Down status¹⁹⁵. Please enter an integer value.</p>

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

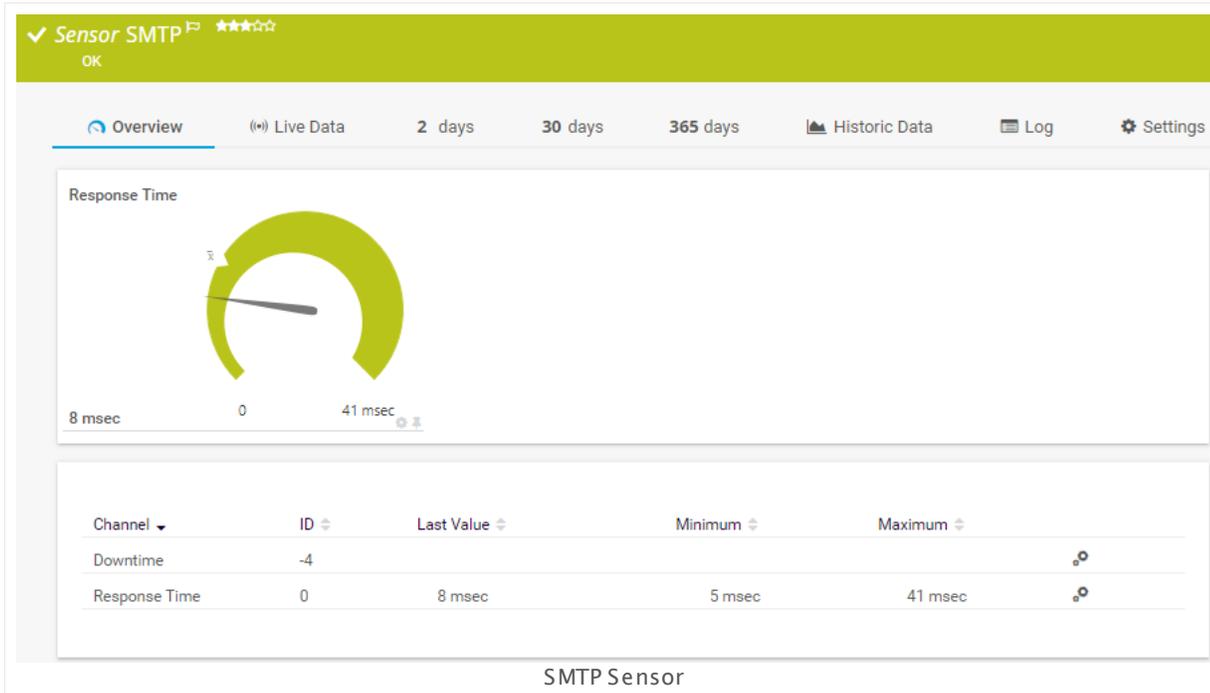
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.121 SMTP Sensor

The SMTP sensor monitors a mail server using Simple Mail Transfer Protocol (SMTP) and can optionally send a test email with every check.

- It shows the response time of the server.



Remarks

- This sensor type does not support Secure Remote Password (SRP) ciphers.
- ☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SMTP SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port that the sensor uses to send an email via SMTP. For non-secure connections usually port 25 is used, for SSL/TLS connections port 465 or 587 . The actual setting depends on the server you connect to.

SMTP SPECIFIC

If you do not get a connection, try another port number.

Please enter an integer value. We recommend that you use the default value.

AUTHENTICATION

Type	Select whether to use an authentication method for the SMTP connection. Choose between: <ul style="list-style-type: none">▪ None: Do not use any authentication method.▪ Username and password: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.
HELO Ident	Enter a server name for the HELO part of the email protocol. For some mail servers, the HELO identifier must be the valid principal host domain name for the client host. See SMTP RFC 2821 .

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: <ul style="list-style-type: none">▪ Use Transport-Level Security if available using StartTLS (default): Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.▪ Use Transport-Level Security if available: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.▪ Enforce Transport-Level Security using StartTLS: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a Down status ¹⁹⁵.
-----------------	--

TRANSPORT-LEVEL SECURITY

- **Enforce Transport-Level Security:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down status**^[195].
- ⓘ If the sensor connects to a server via **StartTLS**, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.
- ⓘ If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

MONITORING

Send Email	Define the monitoring approach when connecting to the SMTP server. Choose between: <ul style="list-style-type: none"> ▪ None: Do not send an email, just connect to the SMTP server. ▪ Send Email: Send an email through the SMTP server. If there is an error when sending the email, an error message will be triggered and the sensor will change to a Down status^[195].
From	Specify the address that the sent emails contain in the from field. Please enter a valid email address.
To	Specify the address that PRTG sends the emails to. If you define more than one recipient, separate the individual email addresses with commas. Please enter a valid email address.
Topic	Specify the subject that the sent emails contain. Please enter a string or leave the field empty.
Content	Specify the body that the sent emails contain. Please enter a string or leave the field empty.
Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result.

MONITORING

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

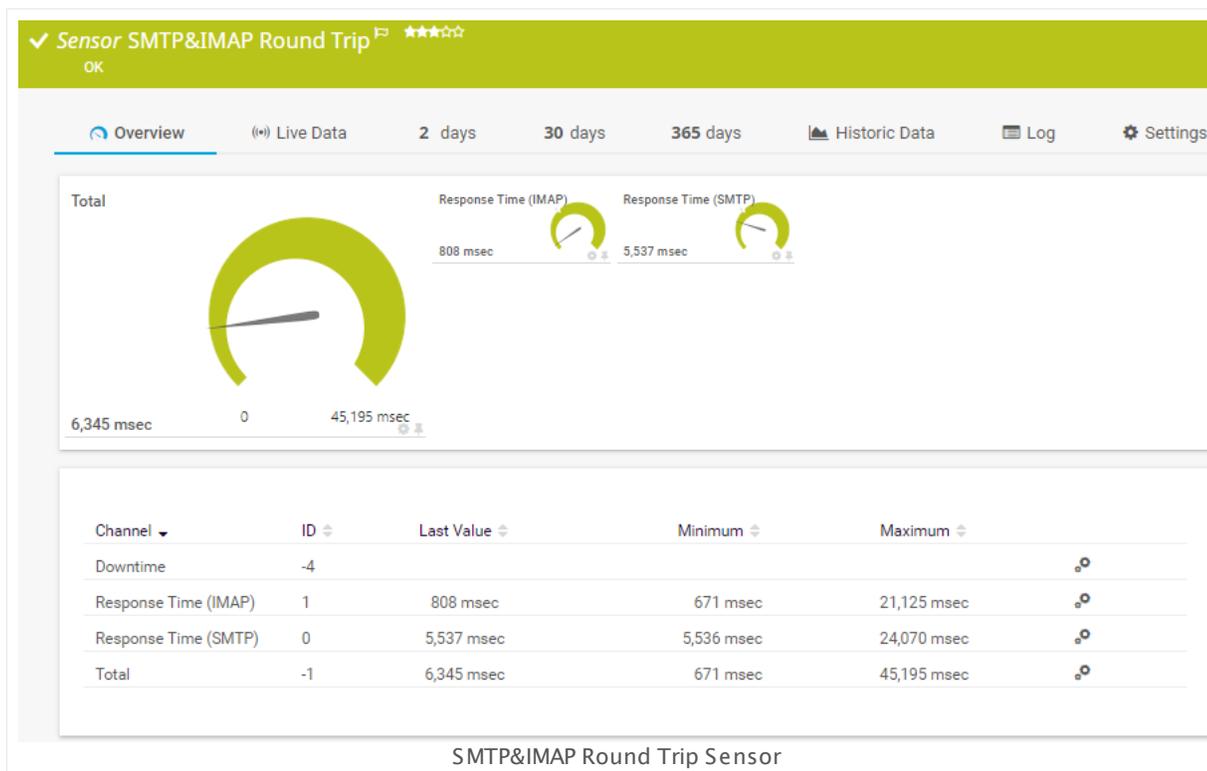
7.8.122 SMTP&IMAP Round Trip Sensor

The SMTP&IMAP Round Trip sensor monitors the time it takes for an email to reach an Internet Message Access Protocol (IMAP) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email using the parent device as SMTP server and then scans a dedicated IMAP mailbox until this email comes in.

The SMTP&IMAP Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor runtime.

The sensor shows the following:

- Response time of SMTP server
- Response time of IMAP server
- Sum of both response times



Sensor in Other Languages

Dutch: **SMTP & IMAP Round Trip**, French: **Durée de boucle SMTP&IMAP**, German: **SMTP&IMAP-Übermittlung**, Japanese: **SMTP&IMAP ? ? ? ? ? ? ?**, Portuguese: **SMTP&IMAP Viagem de ida e volta**, Russian: **Цикл SMTP&IMAP**, Simplified Chinese: **SMTP ? IMAP ? ?**, Spanish: **SMTP&IMAP Round Trip**

Remarks

- Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- For a general introduction to the technology behind round trip monitoring, please see [Monitoring Email Round Trip](#) section.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- ⓘ We recommend that you add this sensor to an SMTP server device only, because the settings of this sensor type are optimized for this scenario.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMAIL SETTINGS

From Specify the address that the sent emails will contain in the from field. Please enter a valid email address.

To Specify the address that PRTG sends the emails to. Please enter a valid email address.

HELO Ident Enter a server name for the HELO part of the mail protocol. For some mail servers the HELO identifier must be the valid principal host domain name for the client host. See [SMTP RFC 2821](#).

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

i In this step, you configure how PRTG sends the emails. As SMTP server, the sensor uses the **IP Address/DNS Name** of the device you add this sensor to.

Port Enter the number of the port that the sensor uses to send an email via SMTP.

For non-secure connections, usually port **25** is used, for SSL/TLS connections port **465** or **587**. The actual setting depends on the server you are connecting to.

If you do not get a connection, please try another port number.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

	Please enter an integer value. We recommend that you use the default value.
Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
SMTP Authentication Type	Define if you want to use authentication for the SMTP connection. Choose between: <ul style="list-style-type: none">▪ None: Do not use any authentication method.▪ Username/Password: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.
Additional Text for Email Subject	<p>The subject part of the round trip email is created automatically by PRTG. It consists of the string PRTG Roundtrip Mail:, followed by a unique GUID to correctly identify the email in the IMAP mailbox, for example, PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}.</p> <p>Use this field to place your custom text before the automatically created text.</p>

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: <ul style="list-style-type: none">▪ Use Transport-Level Security if available using StartTLS (default): Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.▪ Use Transport-Level Security if available: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.
-----------------	--

TRANSPORT-LEVEL SECURITY

- **Enforce Transport-Level Security using StartTLS:** Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a **Down status**¹⁹⁵.
 - **Enforce Transport-Level Security:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down status**¹⁹⁵.
- ⓘ If the sensor connects to a server via **StartTLS**, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.
- ⓘ If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

STEP 2: CHECK AN IMAP MAILBOX UNTIL EMAIL ARRIVES

ⓘ In this step, you configure how to receive the sent emails.

IP Address/DNS Name	Specify the IMAP server. Enter a valid IP address or DNS name.
Mailbox	Specify the IMAP mailbox you want to check. Enter the IMAP mailbox or folder name.
Port	Specify the port that the sensor will use for the IMAP connection. For non-secure connections usually port 143 is used, for SSL/TLS connections port 993 . The actual setting depends on the server you connect to. If you do not get a connection, try another port number. Please enter an integer value. We recommend that you use the default value.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will repeatedly check the mailbox in this interval until the email arrives. Please enter an integer value.

STEP 2: CHECK AN IMAP MAILBOX UNTIL EMAIL ARRIVES

Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will continuously check the mailbox in the interval that you specify above until the email arrives. If it does not arrive within the maximum trip time, the sensor will show an error message. Please enter an integer value.
Username	Enter a username for IMAP authentication. Please enter a string.
Password	Enter a password for IMAP authentication. Please enter a string.
Search Method	Define how to search for the roundtrip email in the mailbox. Choose between: <ul style="list-style-type: none"> ▪ Search email directly (default): Send a SEARCH command to find the roundtrip email directly on the IMAP server. ▪ Search through all available emails: Iterate over all available message in the mailbox on the IMAP server to find the roundtrip email.

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: <ul style="list-style-type: none"> ▪ Use Transport-Level Security if available using StartTLS (default): Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption. ▪ Use Transport-Level Security if available: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption. ▪ Enforce Transport-Level Security using StartTLS: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a Down status¹⁹⁵. ▪ Enforce Transport-Level Security: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a Down status¹⁹⁵. <p>i If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.</p>
-----------------	--

TRANSPORT-LEVEL SECURITY

-  If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

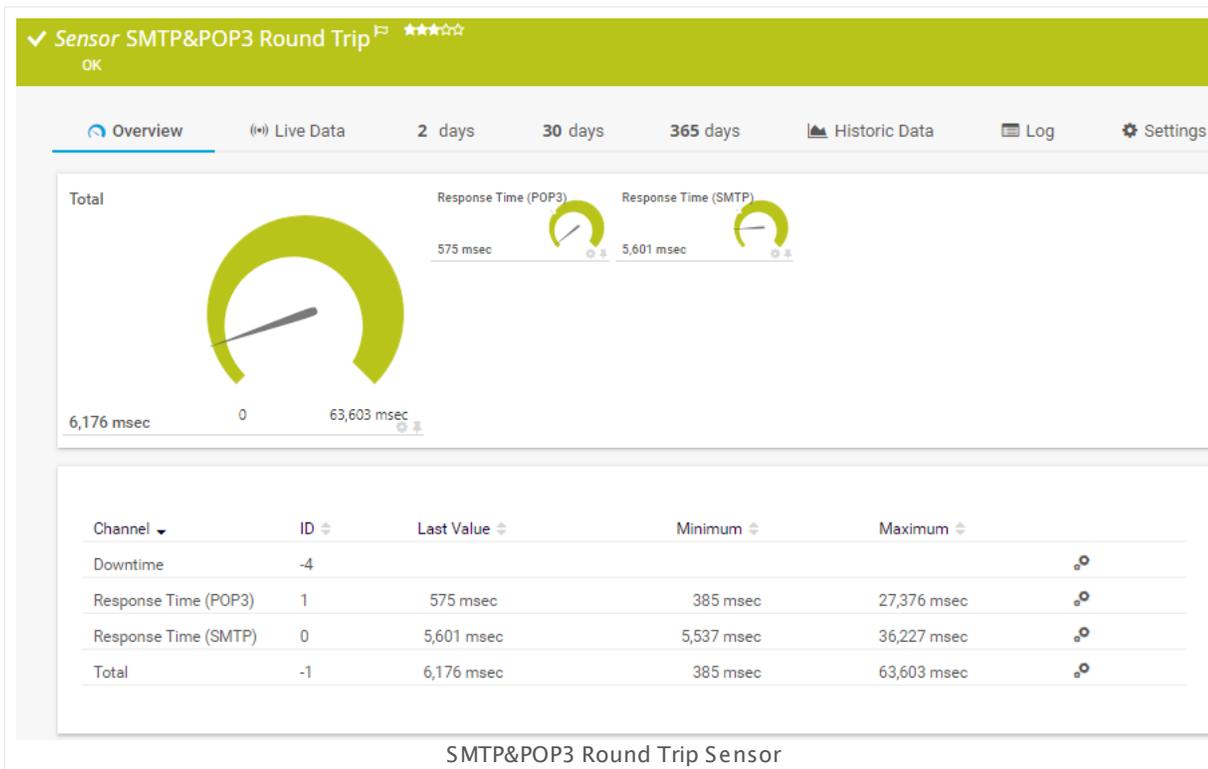
7.8.123 SMTP&POP3 Round Trip Sensor

The SMTP&POP3 Round Trip sensor monitors the time it takes for an email to reach a Post Office Protocol version 3 (POP3) mailbox after being sent using Simple Mail Transfer Protocol (SMTP). It sends an email using the parent device as SMTP server and then scans a dedicated POP3 mailbox until the email comes in.

The SMTP&POP3 Round Trip sensor will delete these emails automatically from the mailbox as soon as PRTG retrieves them. Emails will only remain in the mailbox particularly if a timeout or a restart of the PRTG server occurred during sensor runtime.

The sensor shows the following:

- Response time of SMTP server
- Response time of POP3 server
- Sum of both response times



Sensor in Other Languages

Dutch: **SMTP & POP3 Round Trip**, French: **Durée de boucle SMTP&POP3**, German: **SMTP&POP3-Übermittlung**, Japanese: **SMTP&POP3 ? ? ? ? ? ? ? ?**, Portuguese: **SMTP&POP3 Viagem de ida e volta**, Russian: **Цикл SMTP и POP3**, Simplified Chinese: **SMTP ? POP3 ? ?**, Spanish: **SMTP&POP3 Round Trip**

Remarks

- Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.
- This sensor type does not support Secure Remote Password (SRP) ciphers.
- For a general introduction to the technology behind round trip monitoring, please see [Monitoring Email Round Trip](#) section.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

- ⓘ We recommend that you add this sensor to an SMTP server device only, because the settings of this sensor type are optimized for this scenario.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

EMAIL SETTINGS

From Specify the address that the sent emails will contain in the from field. Please enter a valid email address.

To Specify the address that PRTG sends the emails to. Please enter a valid email address.

HELO Ident Enter a server name for the HELO part of the mail protocol. For some mail servers the HELO identifier must be the valid principal host domain name for the client host. See [SMTP RFC 2821](#).

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

 In this step, you configure how PRTG sends the emails. As SMTP server, the sensor uses the **IP-Address/DNS Name** of the device you add this sensor to.

Port Enter the number of the port that the sensor uses to send an email via SMTP.

For non-secure connections usually port 25 is used, for SSL/TLS connections port 465 or 587. The actual setting depends on the server you connect to.

If you do not get a connection, try another port number.

Please enter an integer value. We recommend that you use the default value.

STEP 1: SEND EMAIL WITH PARENT DEVICE AS SMTP SERVER

Timeout for SMTP Connection (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
SMTP Authentication Type	Define if you want to use an authentication for the SMTP connection. Choose between: <ul style="list-style-type: none">▪ None: Do not use any authentication method.▪ Username/Password: Authenticate at the SMTP server via username and password.
Username	This field is only visible if you enable SMTP authentication above. Enter a username for SMTP authentication. Please enter a string.
Password	This field is only visible if you enable SMTP authentication above. Enter a password for SMTP authentication. Please enter a string.
Additional Text for Email Subject	<p>The subject part of the round trip email is created automatically by PRTG. It consists of the string PRTG Roundtrip Mail:, followed by a unique GUID to correctly identify the email in the POP3 mailbox, for example, PRTG Roundtrip Mail: {5E858D9C-AC70-466A-9B2A-55630165D276}.</p> <p>Use this field to place your custom text before the automatically created text.</p>

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: <ul style="list-style-type: none">▪ Use Transport-Level Security if available using Start TLS (default): Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption.▪ Use Transport-Level Security if available: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption.▪ Enforce Transport-Level Security using Start TLS: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a Down status¹⁹⁵.
-----------------	---

TRANSPORT-LEVEL SECURITY

- **Enforce Transport-Level Security:** Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a **Down status** ¹⁹⁵.
- ① If the sensor connects to a server via **StartTLS**, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.
- ① If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

STEP 2: CHECK A POP3 MAILBOX UNTIL EMAIL ARRIVES

- ① In this step, you configure how to receive the sent emails.

IP Address/DNS Name	Specify the POP3 server. Enter a valid IP address or DNS name.
Port	Specify the port that the sensor uses for the POP3 connection. For non-secure connections usually port 110 is used, for SSL/TLS connections port 995 . The actual setting depends on the server you are connecting to. If you do not get a connection, please try another port number. Please enter an integer value. We recommend that you use the default value.
Connection Interval (Sec.)	Enter the number of seconds the sensor will wait between two connections to the IMAP server. PRTG will continuously check the mailbox in this interval until the email arrives. Please enter an integer value.
Maximum Trip Time (Sec.)	Enter the number of seconds an email may take to arrive in the IMAP mailbox. PRTG will continuously check the mailbox in the interval that you specify above until the email arrives. If it does not arrive within the maximum trip time, the sensor will trigger an error message. Please enter an integer value.

STEP 2: CHECK A POP3 MAILBOX UNTIL EMAIL ARRIVES

POP3 Authentication Type	Select the kind of authentication for the POP3 connection. Choose between: <ul style="list-style-type: none"> ▪ Without Login: Monitor the connection to the POP3 server only. ▪ Username and Password: Log in into the POP3 server with username and password (simple login, non-secure). ▪ 128-bit MD5 hash value (APOP): Send the password in an encrypted form using APOP. This option must be supported by the POP3 server you connect to.
Username	This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.
Password	This field is only visible if you select an option with login above. Enter a username for POP3 authentication. Please enter a string.

TRANSPORT-LEVEL SECURITY

Sensor Specific	Define the security level for the sensor connection. Choose between: <ul style="list-style-type: none"> ▪ Use Transport-Level Security if available using StartTLS (default): Choose this option to try to connect to the server using TLS and StartTLS. If the server does not support this, the sensor will try to connect without encryption. ▪ Use Transport-Level Security if available: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will try to connect without encryption. ▪ Enforce Transport-Level Security using StartTLS: Choose this option to try connecting to the server using TLS and StartTLS. If the server does not support this, the sensor will show a Down status^[195]. ▪ Enforce Transport-Level Security: Choose this option to try to connect to the server using TLS. If the server does not support this, the sensor will show a Down status^[195]. <p>i If the sensor connects to a server via StartTLS, the connection is established unencrypted first. After the connection is established, the sensor sends a certain command (StartTLS) over the unencrypted connection to negotiate a secure connection via the SSL/TLS protocol.</p>
-----------------	--

TRANSPORT-LEVEL SECURITY

-  If the sensor uses **TLS without StartTLS**, the negotiation of a secure connection happens immediately (implicitly) so that no commands are sent in unencrypted plain text. If there is no secure connection possible, no communication will take place.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default)**: Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.124 SNMP APC Hardware Sensor

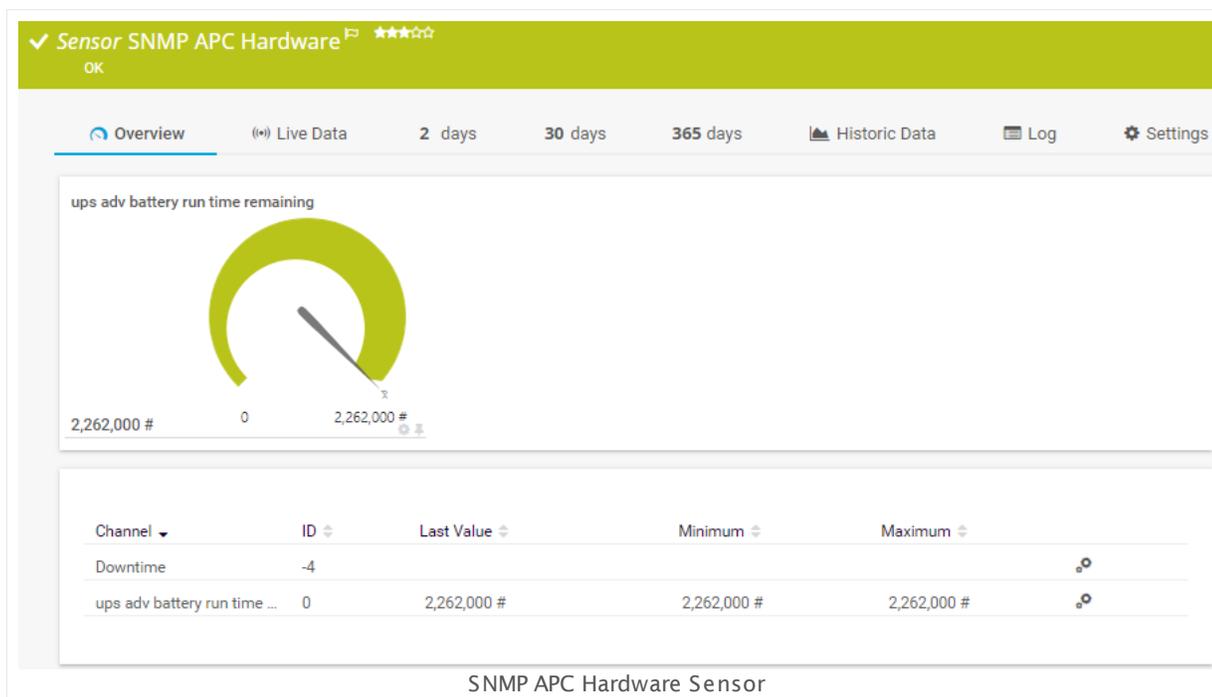
The SNMP APC Hardware sensor monitors performance counters on an APC UPS device using Simple Network Management Protocol (SNMP).

It can show the following:

- Actual voltage of battery
- Capacity of battery
- Temperature of battery
- Remaining runtime of battery
- Input and output frequency
- Input and output voltage
- Output load

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

i The SNMP APC Hardware sensor will not appear as running sensor, instead it will be created as [SNMP Custom Advanced sensor](#).



Sensor in Other Languages

Dutch: **SNMP APC Hardware**, French: **Matériels SNMP APC**, German: **SNMP APC Hardware**, Japanese: **SNMP APC** ? ? ? ? ? , Portuguese: **Hardware SNMP APC**, Russian: **Оборудование SNMP APC**, Simplified Chinese: **SNMP APC** ? ? , Spanish: **SNMP APC Hardware**

Remarks

- Knowledge Base: [How can I monitor additional counters with the SNMP APC Hardware sensor?](#)
- Knowledge Base: [How can I monitor an APC UPS that does not support SNMP?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters you want to monitor. PRTG will create one [SNMP Custom Advanced sensor](#) for each Library OID category you select in the **Add Sensor** dialog. If you select more than 10 OIDs per category, PRTG will create the corresponding amount of SNMP Custom Advanced sensors. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

APC UPS SPECIFIC

Library OIDs	Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

APC UPS SPECIFIC

Selected Interface	Shows the name of the interface (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that the sensor monitors at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the quotient here. Please enter an integer value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer value.

APC UPS SPECIFIC

- If Value Changes Define what this sensor will do when the sensor value changes. You can choose between:
- **Ignore changes (default):** The sensor takes no action on change.
 - **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) 3170 whenever the sensor value changes.

SENSOR DISPLAY

- Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- i** You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
- i** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) 3160 settings).
- Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I monitor additional counters with the SNMP APC Hardware sensor?

- <https://kb.paessler.com/en/topic/60367>

Knowledge Base: How can I monitor an APC UPS that does not support SNMP?

- <https://kb.paessler.com/en/topic/63674>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.125 SNMP Buffalo TS System Health Sensor

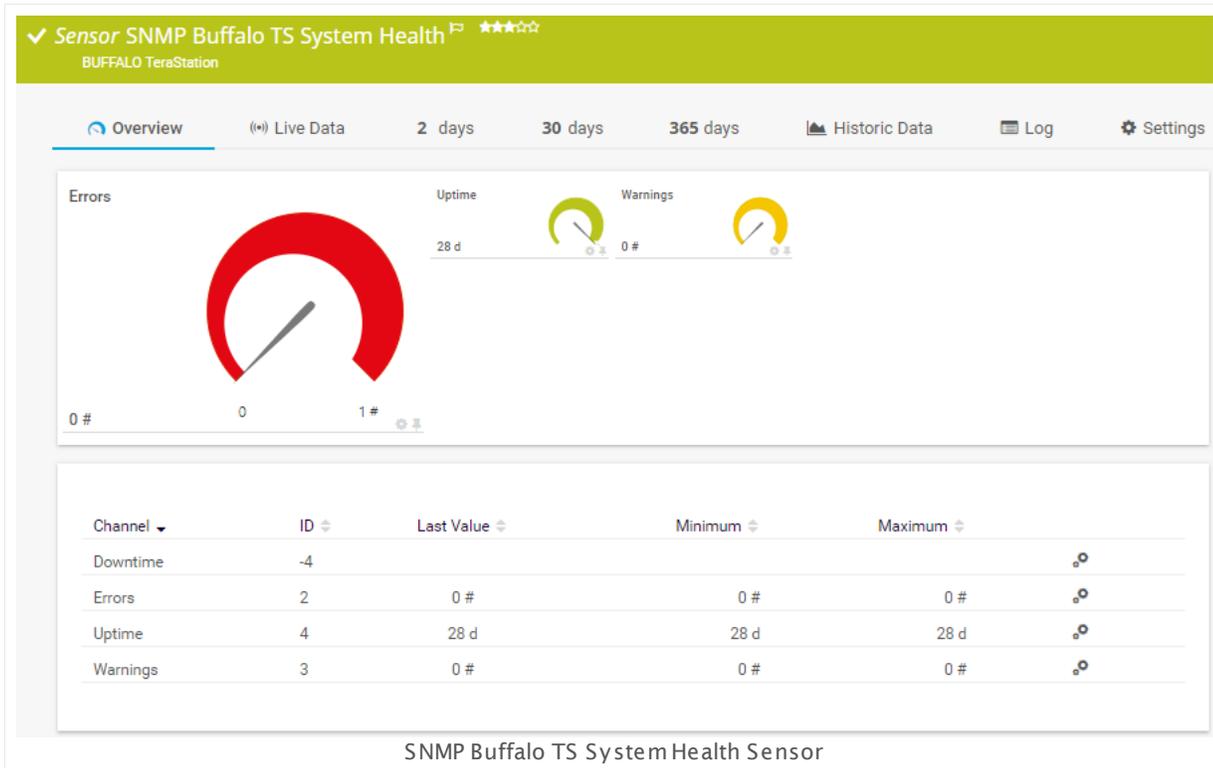
The SNMP Buffalo TS System Health sensor monitors the system health of a Buffalo TeraStation Network Attached Storage (NAS) using Simple Network Management Protocol (SNMP). Supported TeraStation systems are the 3000, 3010, 5000, 5010, and 7000 series.

It can show the following:

- Number of errors
- Number of warnings
- Available memory in total and percent
- CPU usage
- Uptime
- Failover status: idle, busy, starting main, starting backup, initializing, stopping
- Firmware update availability: yes, no, unknown
- RPSU status: fine, broken, unknown

The channels are created at run-time, depending on your Buffalo TeraStation NAS and firmware version. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

 Run an [Auto-Discovery](#)^[282] with the device template **Buffalo TeraStation NAS** to automatically create [SNMP Custom Table sensors](#)^[1992] with additional useful information about your Buffalo TeraStation, for example, array status, disk smart status, disk status, and iSCSI status. This device template will also create [SNMP sensors](#)^[431] for traffic, memory, and load average on your TeraStation.



Sensor in Other Languages

Dutch: **SNMP Buffalo TS System Status**, French: **État du système SNMP Buffalo TS**, German: **SNMP Buffalo TS System Health**, Japanese: **SNMP Buffalo TS System? ? ?**, Portuguese: **SNMP Buffalo TS Funcionamento do sistema**, Russian: **Работоспособность системы Buffalo TS no SNMP**, Simplified Chinese: **SNMP Buffalo TS ? ? ? ? ?**, Spanish: **Salud del sistema NS de Buffalo TS SNMP**

Remarks

- This sensor supports the TeraStation 3000, 3010, 5000, 5010, and 7000 series.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)^[3180].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
125 SNMP Buffalo TS System Health Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

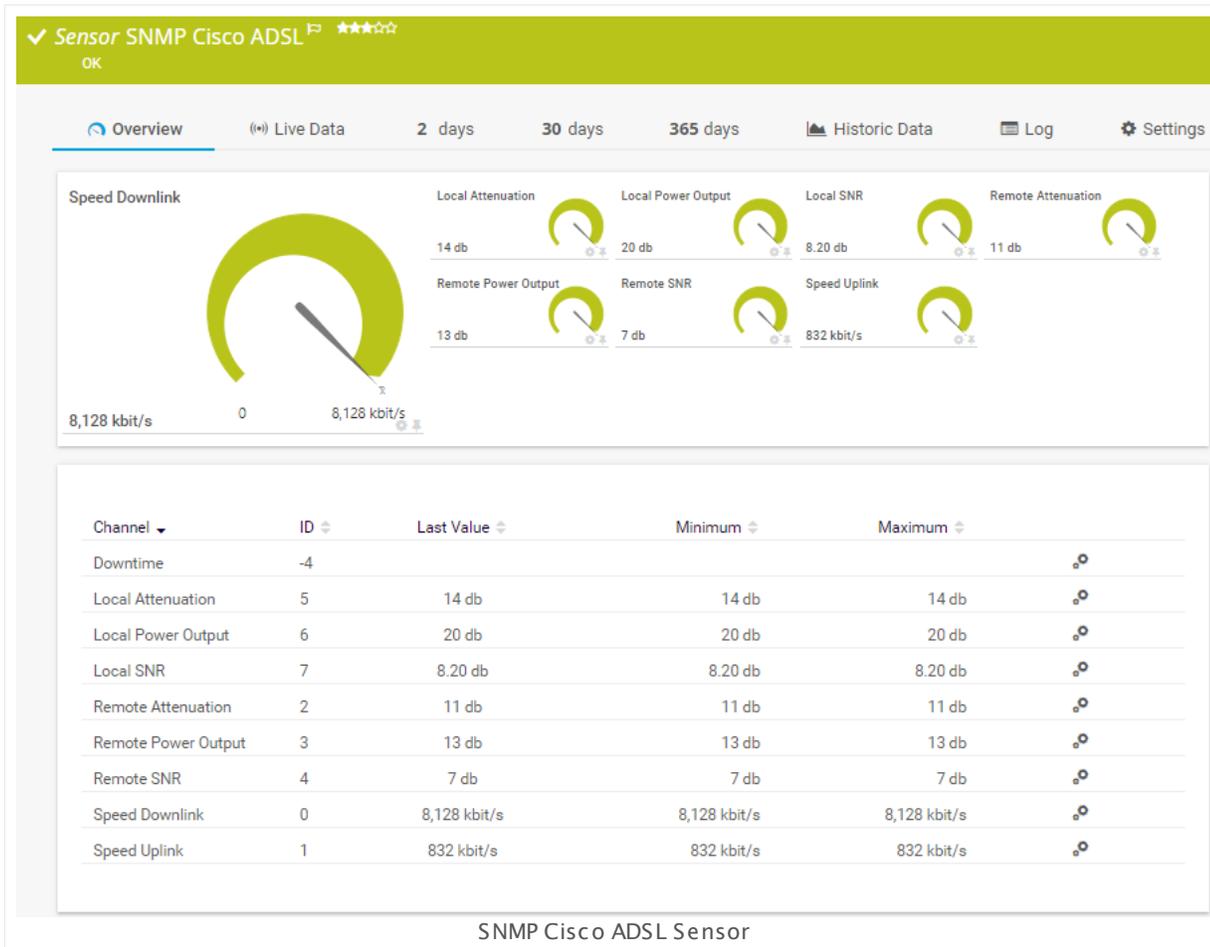
7.8.126 SNMP Cisco ADSL Sensor

The SNMP Cisco ADSL sensor monitors Asymmetric Digital Subscriber Line (ADSL) statistics of a Cisco router using Simple Network Management Protocol (SNMP).

It shows the following:

- Speed of downlink
- Speed of uplink
- Remote and local attenuation
- Remote and local SNR (signal-to-noise ratio)
- Remote and local power output

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters you want to monitor. PRTG will create one sensor for each counter you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CISCO ADSL SETTINGS

Line Index	Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.127 SNMP Cisco ASA VPN Connections Sensor

The SNMP Cisco ASA VPN Connections sensor monitors the Virtual Private Network (VPN) connections on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP).

It can show the following:

- Active email sessions
- Active Internet Protocol Security (IPsec) sessions
- Active L2L sessions
- Active LB sessions
- Active sessions in total
- Active SVC sessions
- Active users
- Groups with active users

✓ Sensor SNMP Cisco ASA VPN Connections ★★★★☆

OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Active Sessions

0 #

Active Email Sessions

0 #

Active IPsec Sessions

0 #

Active L2L Sessions

1 #

Active LB Sessions

0 #

Active SVC Sessions

0 #

Active Users

0 #

Active WebVPN Sessio

0 #

Groups With Active Us

0 #

Channel	ID	Last Value	Minimum	Maximum	
Active Email Sessions	3	0 #	0 #	0 #	
Active IPsec Sessions	4	0 #	0 #	0 #	
Active L2L Sessions	5	1 #	1 #	1 #	
Active LB Sessions	6	0 #	0 #	0 #	
Active Sessions	0	0 #	0 #	0 #	
Active SVC Sessions	7	0 #	0 #	0 #	
Active Users	1	0 #	0 #	0 #	
Active WebVPN Sessions	8	0 #	0 #	0 #	
Downtime	-4				
Groups With Active Users	2	0 #	0 #	0 #	

SNMP Cisco ASA VPN Connections Sensor

Sensor in Other Languages

Dutch: **SNMP Cisco ASA VPN Verbindingen**, French: **Connexions VPN ASA Cisco SNMP**, German: **SNMP Cisco ASA VPN-Verbindungen**, Japanese: **SNMP Cisco ASA VPN ? ? ?** , Portuguese: **Conexões VPN SNMP Cisco ASA**, Russian: **Подключения SNMP Cisco ASA VPN**, Simplified Chinese: **SNMP Cisco ASA VPN ? ?** , Spanish: **Conexiones SNMP Cisco ASA VPN**

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

SNMP Version	<p>Select the SNMP version for the device connection. Choose between:</p> <ul style="list-style-type: none"> ▪ v1: Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices. <ul style="list-style-type: none">  SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP. ▪ v2c (recommended): Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters. ▪ v3: Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption. <ul style="list-style-type: none">  When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased Interval Delay or Open Requests with the Probe Health Sensor^[1590], distribute the load over multiple probes^[3709]. SNMP v1 and v2 do not have this limitation.
Community String	<p>This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.</p>
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication.

CREDENTIALS FOR SNMP DEVICES

The type you choose must match the authentication type of your device.

i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field **Password** empty. In this case, **SNMP_SEC_LEVEL_NOAUTH** is used and authentication deactivated entirely.

User This setting is only visible if you select SNMP version **v3** above. Enter a username for secure authentication. This value must match the username of your device.

Password This setting is only visible if you select SNMP version **v3** above. Enter a password for secure authentication. This value must match the password of your device.

Encryption Type This setting is only visible if you select SNMP version **v3** above. Select an encryption type. Choose between:

- **DES**: Use **Data Encryption Standard** (DES) as encryption algorithm.
- **AES**: Use **Advanced Encryption Standard** (AES) as encryption algorithm.

i AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.

i The type that you choose must match the encryption type of your device.

Data Encryption Key This setting is only visible if you select SNMP version **v3** above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.

i If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.

Context Name This setting is only visible if you select SNMP version **v3** above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.

SNMP Port Enter the port for the SNMP communication. We recommend that you use the default value.

CREDENTIALS FOR SNMP DEVICES

SNMP Timeout (Sec.) Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is **300** seconds (5 minutes).

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[336] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

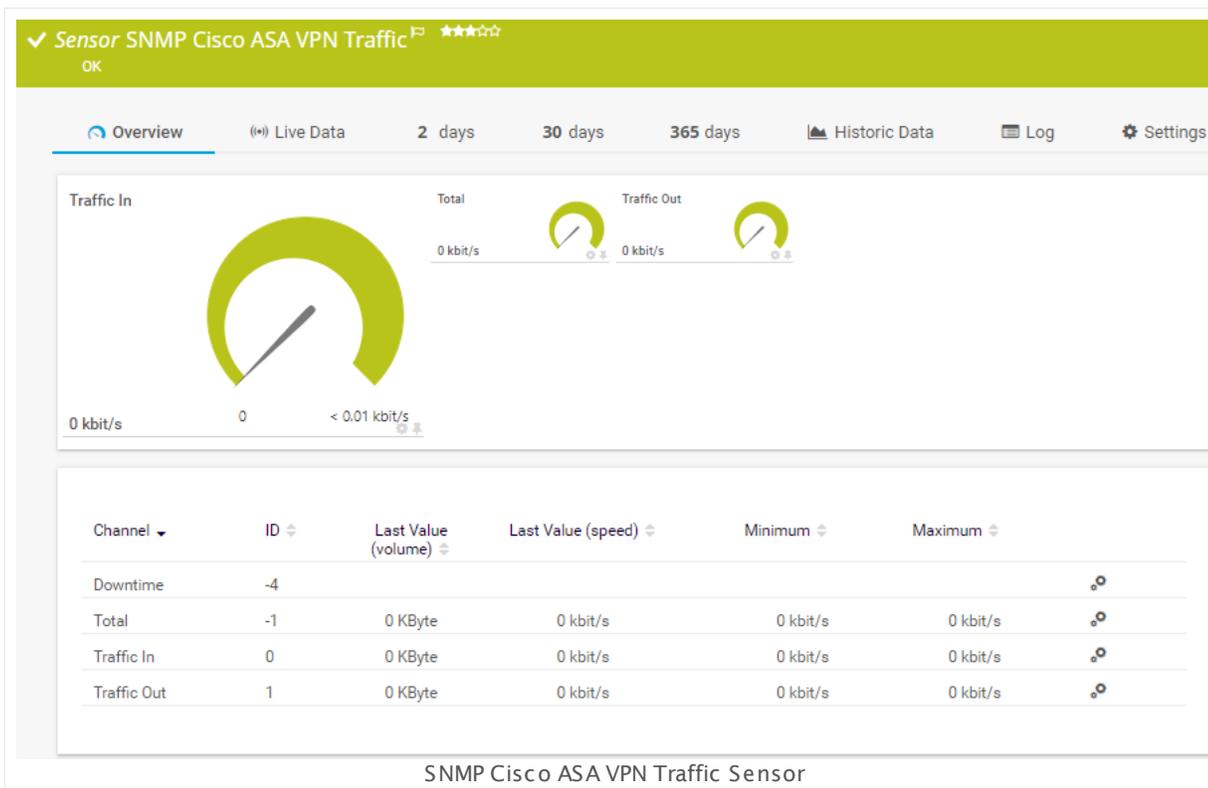
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.128 SNMP Cisco ASA VPN Traffic Sensor

The SNMP Cisco ASA VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) connection on a Cisco Adaptive Security Appliance using Simple Network Management Protocol (SNMP).

It shows the following:

- Incoming traffic
- Outgoing traffic



Sensor in Other Languages

Dutch: **SNMP Cisco ASA VPN Verkeer**, French: **Traffic VPN ASA Cisco SNMP**, German: **SNMP Cisco ASA VPN-Datenverkehr**, Japanese: **SNMP Cisco ASA VPN**, Portuguese: **Tráfego VPN SNMP Cisco ASA**, Russian: **Трафик SNMP Cisco ASA VPN**, Simplified Chinese: **SNMP Cisco ASA VPN**, Spanish: **Trafico SNMP Cisco ASA VPN**

Remarks

- This sensor type is intended to monitor permanent connections. It will show an error if a connection is interrupted.
- This sensor can monitor IPsec connections only!
- Knowledge Base: [I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?](#)

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the connections you want to monitor. PRTG will create one sensor for each connection you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

ASA VPN SPECIFIC

Connections Select the IPsec VPN connections you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 This sensor type can only monitor VPN connections based on **IPsec**. This means, for example, that connections using **Cisco AnyConnect** are not listed here.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)

BASIC SENSOR SETTINGS



Parent Tags

Shows **Tags** that this sensor inherits from its parent device, group, and probe. This setting is shown for your information only and cannot be changed here.

Tags

Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ASA VPN SPECIFIC

Remote IP

Shows the IP address of the connection this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

i This sensor type can only monitor VPN connections based on **IPsec**.

Sensor Behavior

Define the **status of the sensor** if there is no active connection available. Choose between:

- **Show 'Down' status if no connection is active (recommended)**
- **Show 'Warning' status if no connection is active**
- **Stay in 'Up' status if no connection is active**

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	Select the SNMP version for the device connection. Choose between:
--------------	--

CREDENTIALS FOR SNMP DEVICES

- **v1:** Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

i SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP.

- **v2c (recommended):** Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.

- **v3:** Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

i When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased **Interval Delay** or **Open Requests** with the **Probe Health Sensor**, distribute the load over **multiple probes**. SNMP v1 and v2 do not have this limitation.

Community String	This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <p>i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.</p>
User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.

CREDENTIALS FOR SNMP DEVICES

Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)  for more

SCANNING INTERVAL

information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: I get the error PE123 when using the SNMP Cisco ASA VPN Traffic sensor. What can I do?

- <https://kb.paessler.com/en/topic/59643>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
128 SNMP Cisco ASA VPN Traffic Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

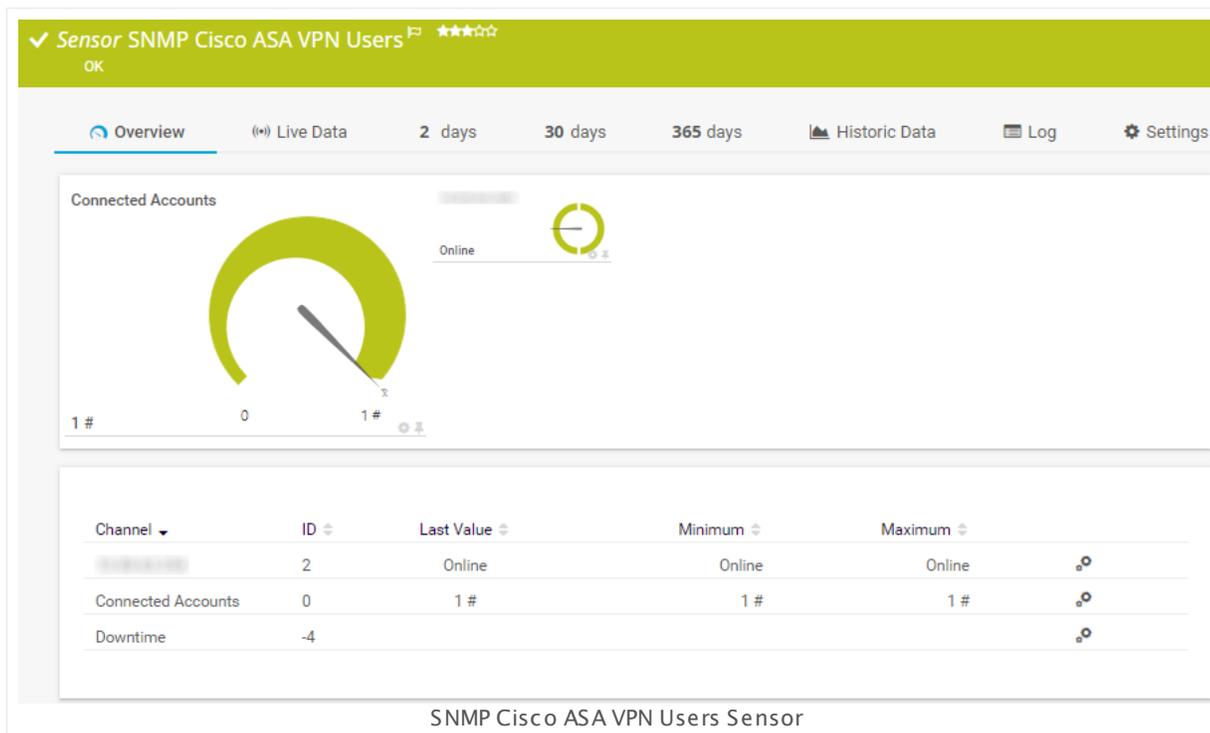
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.129 SNMP Cisco ASA VPN Users Sensor

The SNMP Cisco ASA VPN Users sensor monitors account connections to a Virtual Private Network (VPN) on a Cisco Adaptive Security Appliance via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of currently connected accounts
- If a specific user account is currently offline or online



Sensor in Other Languages

Dutch: **SNMP Cisco ASA VPN Gebruikers**, French: **Utilisateurs Cisco ASA VPN SNMP**, German: **SNMP Cisco ASA VPN-Benutzer**, Japanese: **SNMP Cisco ASA VPN ? ? ? ?**, Portuguese: **Usuários VPN SNMP Cisco ASA**, Russian: **Пользователи SNMP Cisco ASA VPN**, Simplified Chinese: **SNMP Cisco ASA VPN ? ?**, Spanish: **Usuarios de SNMP Cisco ASA VPN**

Remarks

- Please do not use the sensor to monitor more than 50 VPN users, especially if they are all connected simultaneously. For more information, see this Knowledge Base article: [My Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

CREDENTIALS FOR SNMP DEVICES

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SNMP Version	Select the SNMP version for the device connection. Choose between:
--------------	--

CREDENTIALS FOR SNMP DEVICES

- **v1:** Use the simple v1 protocol for SNMP connections. This protocol only offers clear-text data transmission, but it is usually supported by all devices.

i SNMP v1 does not support 64-bit counters. This may result in invalid data when monitoring traffic via SNMP.

- **v2c (recommended):** Use the more advanced v2c protocol for SNMP connections. This is the most common SNMP version. Data is still transferred as clear-text, but it supports 64-bit counters.

- **v3:** Use the v3 protocol for SNMP connections. It provides secure authentication and data encryption.

i When using SNMP v3 you can only monitor a limited number of sensors per second due to internal limitations. The limit is somewhere between 1 and 50 sensors per second (depending on the SNMP latency of your network). This means that using an interval of 60 seconds limits you to between 60 and 3000 SNMP v3 sensors for each probe. If you experience an increased **Interval Delay** or **Open Requests** with the **Probe Health Sensor**, distribute the load over **multiple probes**. SNMP v1 and v2 do not have this limitation.

Community String	This setting is only visible if you select SNMP version v1 or v2c above. Enter the community string of your devices. This is a kind of "clear-text password" for simple authentication. We recommend that you use the default value.
Authentication Type	<p>This setting is only visible if you select SNMP version v3 above. Choose between:</p> <ul style="list-style-type: none"> ▪ MD5: Use Message-Digest Algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. <p>The type you choose must match the authentication type of your device.</p> <p>i If you do not want to use authentication, but you need SNMP v3, for example, because your device requires context, you can leave the field Password empty. In this case, SNMP_SEC_LEVEL_NOAUTH is used and authentication deactivated entirely.</p>
User	This setting is only visible if you select SNMP version v3 above. Enter a username for secure authentication. This value must match the username of your device.

CREDENTIALS FOR SNMP DEVICES

Password	This setting is only visible if you select SNMP version v3 above. Enter a password for secure authentication. This value must match the password of your device.
Encryption Type	<p>This setting is only visible if you select SNMP version v3 above. Select an encryption type. Choose between:</p> <ul style="list-style-type: none">▪ DES: Use Data Encryption Standard (DES) as encryption algorithm.▪ AES: Use Advanced Encryption Standard (AES) as encryption algorithm. <p> AES 192 and AES 256 are not supported by Net-SNMP. They lack RFC specification.</p> <p> The type that you choose must match the encryption type of your device.</p>
Data Encryption Key	<p>This setting is only visible if you select SNMP version v3 above. Enter an encryption key here. If you provide a key in this field, SNMP data packets are encrypted using the encryption algorithm selected above, which provides increased security. The key that you enter here must match the encryption key of your device.</p> <p> If the key you enter in this field does not match the key configured on the target SNMP device, you will not get an error message about this! Please enter a string or leave the field empty.</p>
Context Name	This setting is only visible if you select SNMP version v3 above. Enter a context name only if it is required by the configuration of the device. Context is a collection of management information accessible by an SNMP device. Please enter a string.
SNMP Port	Enter the port for the SNMP communication. We recommend that you use the default value.
SNMP Timeout (Sec.)	Enter a timeout in seconds for the request. Please enter an integer value. If the reply takes longer than the value you enter here, the request is aborted and an error message triggered. The maximum timeout value is 300 seconds (5 minutes).

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more

SCANNING INTERVAL

information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: My Cisco ASA VPN Users sensor shows a user limit error. Why? What can I do?

- <https://kb.paessler.com/en/topic/64053>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
129 SNMP Cisco ASA VPN Users Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

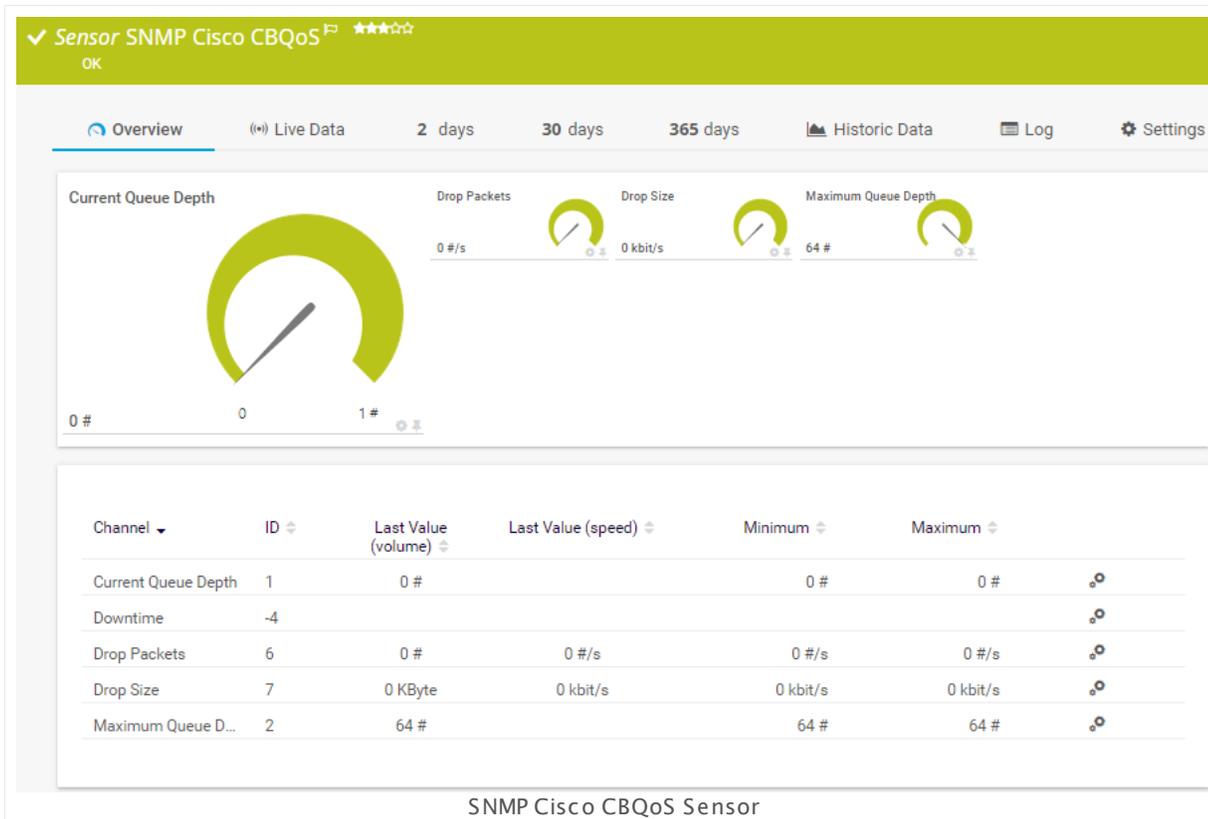
7.8.130 SNMP Cisco CBQoS Sensor

The SNMP Cisco CBQoS sensor monitors network parameters using Cisco's Class Based Quality of Service (CBQoS) via Simple Network Management Protocol (SNMP). It supports the classes Class Map, Match Statement, and Queueing.

The sensor can show the following depending on the particular class type:

- Current and maximum queue depth
- Pre policy packets
- Pre and post policy size
- Drop packets and size
- Drop packets without buffer
- Fragment packets and size.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) [3489].

- For a general introduction to the technology behind Quality of Service monitoring, please see manual section [Monitoring Quality of Service](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the CBQoS entries you want to monitor. To monitor Quality of Service (QoS) via compatible devices, PRTG will create one sensor for each CBQoS entry you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CLASS BASED QOS SPECIFIC

CBQoS Entries	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
---------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
-------------	--

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CLASS BASED QOS SPECIFIC

Object Type	Shows further information about the parameter that this sensor monitors. Once a sensor is created, you cannot change this value.
Interface	It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
BitMask	
ObjectID	
ConfigID	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

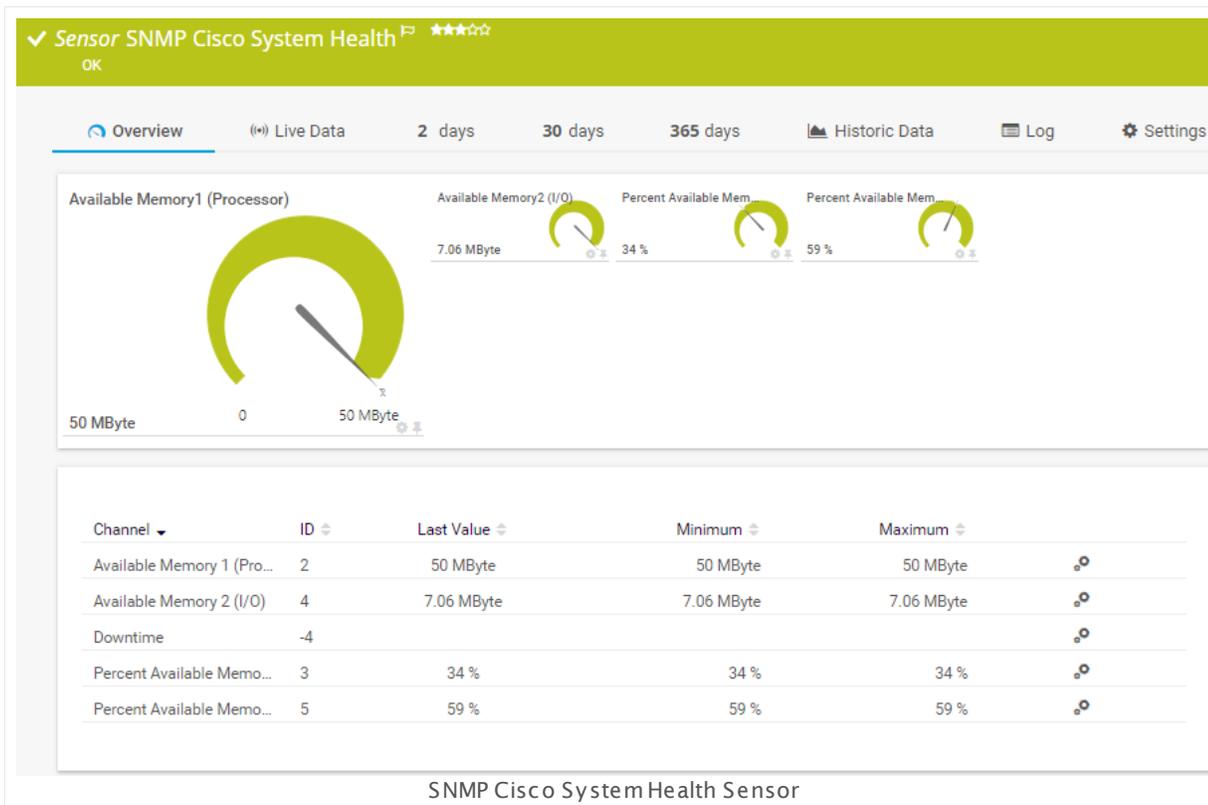
7.8.131 SNMP Cisco System Health Sensor

The SNMP Cisco System Health sensor monitors the system health of a Cisco device via Simple Network Management Protocol (SNMP).

Depending on what your device can deliver via SNMP, the sensor can show, for example, the following system health components:

- CPU load in percent
- Available memory in absolute and percentage values
- Values of the current
- Status of power supplies
- Voltage values
- Fan states
- Current temperature and temperature status
- Other information, for example, transmit and receive power

PRTG creates one sensor per component. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP Cisco System Health**, French: **État du système Cisco SNMP**, German: **SNMP Cisco Systemzustand**, Japanese: **SNMP Cisco ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema SNMP Cisco**, Russian: **Работоспособность системы устройства SNMP Cisco**, Simplified Chinese: **SNMP Cisco ? ? ? ? ? ? ?**, Spanish: **SNMP Salud de sistema Cisco**

Remarks

- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)³¹⁶⁰.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the components you want to monitor. To monitor the system health of a Cisco device, PRTG will create one sensor for each measurement you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CISCO SYSTEM HEALTH SPECIFIC

Measurement	Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CISCO SYSTEM HEALTH SPECIFIC

Measurement	Shows the ID of the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------	---

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

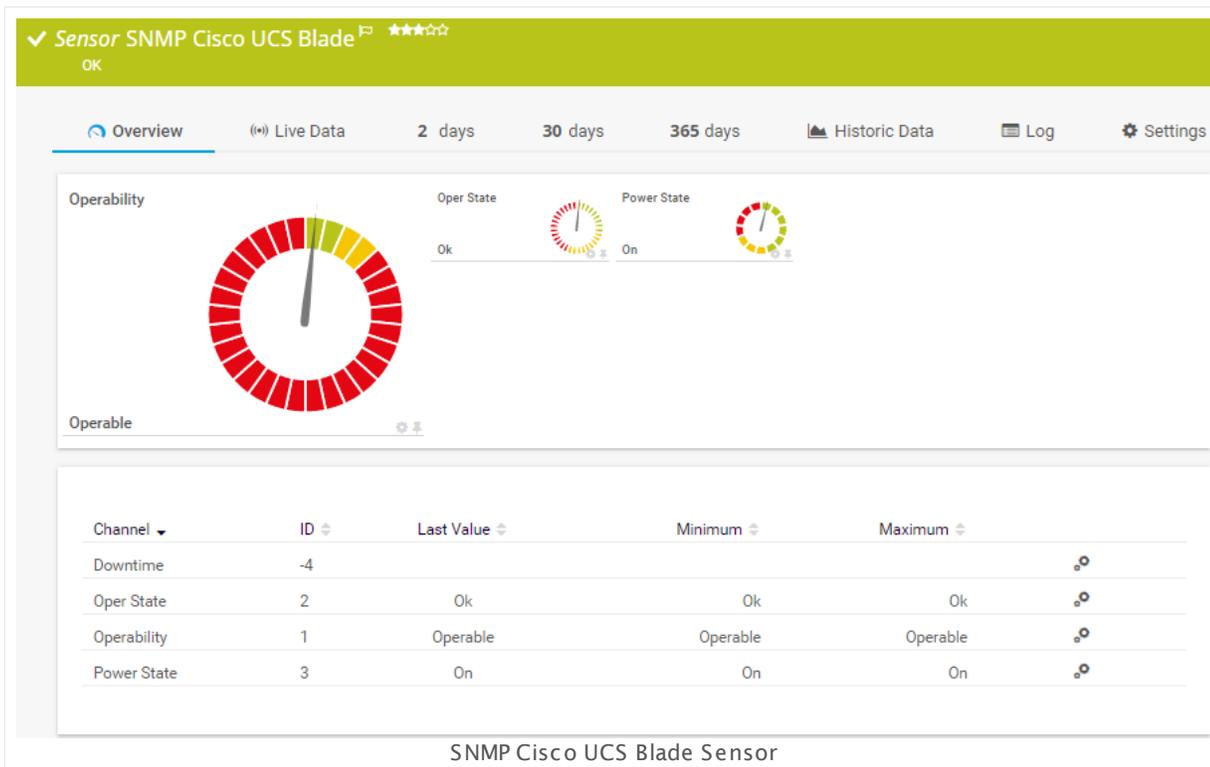
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.132 SNMP Cisco UCS Blade Sensor

The SNMP Cisco UCS Blade sensor monitors the health status of a Cisco Unified Computing System (UCS) blade server via Simple Network Management Protocol (SNMP).

It can show the following states:

- Operability
- Oper state
- Power state



Sensor in Other Languages

Dutch: **SNMP Cisco UCS Blade**, French: **Serveur lame Cisco UCS SNMP**, German: **SNMP Cisco UCS Blade**, Japanese: **SNMP Cisco UCS ? ? ? ?**, Portuguese: **Blade UCS Cisco SNMP**, Russian: **Блейд-сервер SNMP Cisco UCS**, Simplified Chinese: **SNMP Cisco UCS ? ?**, Spanish: **Blade del Cisco UCS del SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the blade servers you want to monitor. PRTG will create one sensor for each blade you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Blade Server Select the blades you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) ^[181], as well as in [alarms](#) ^[213], [logs](#) ^[228], [notifications](#) ^[3216], [reports](#) ^[3262], [maps](#) ^[3270], [libraries](#) ^[3235], and [tickets](#) ^[230].

Parent Tags Shows [Tags](#) ^[139] that this sensor [inherits](#) ^[140] from its [parent device, group, and probe](#) ^[133]. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SENSOR SETTINGS

Blade Server	Shows information about the blade server that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Channel Mask	
Model	
Serial Number	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.133 SNMP Cisco UCS Chassis Sensor

The SNMP Cisco UCS Chassis sensor monitors the health status of the chassis of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the states of the following properties:

- Configuration
- License
- Oper
- Operability
- Power
- Thermal
- Serial electronic erasable programmable read-only memory (SEEPROM)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Channel	ID	Last Value	Minimum	Maximum
Config State	0	Ok	Ok	Ok
Downtime	-4			
License State	1	License Ok	License Ok	License Ok
Oper State	2	Operable	Operable	Operable
Operability	3	Operable	Operable	Operable
Power State	4	Ok	Ok	Ok
Seeprom State	6	Operable	Operable	Operable
Thermal State	5	Ok	Ok	Ok

SNMP Cisco UCS Chassis Sensor

Sensor in Other Languages

Dutch: **SNMP Cisco UCS Chassis**, French: **Châssis SNMP Cisco UCS**, German: **SNMP Cisco UCS Chassis**, Japanese: **SNMP Cisco UCS** ? ? ? ? , Portuguese: **Chassi UCS Cisco SNMP**, Russian: **Копныс SNMP Cisco UCS**, Simplified Chinese: **SNMP Cisco UCS** ? ? , Spanish: **Carcasa del Cisco UCS del SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the chassis you want to monitor. PRTG will create one sensor for each chassis you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Chassis	Select the chassis you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
---------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Chassis	Shows the chassis that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
---------	---

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

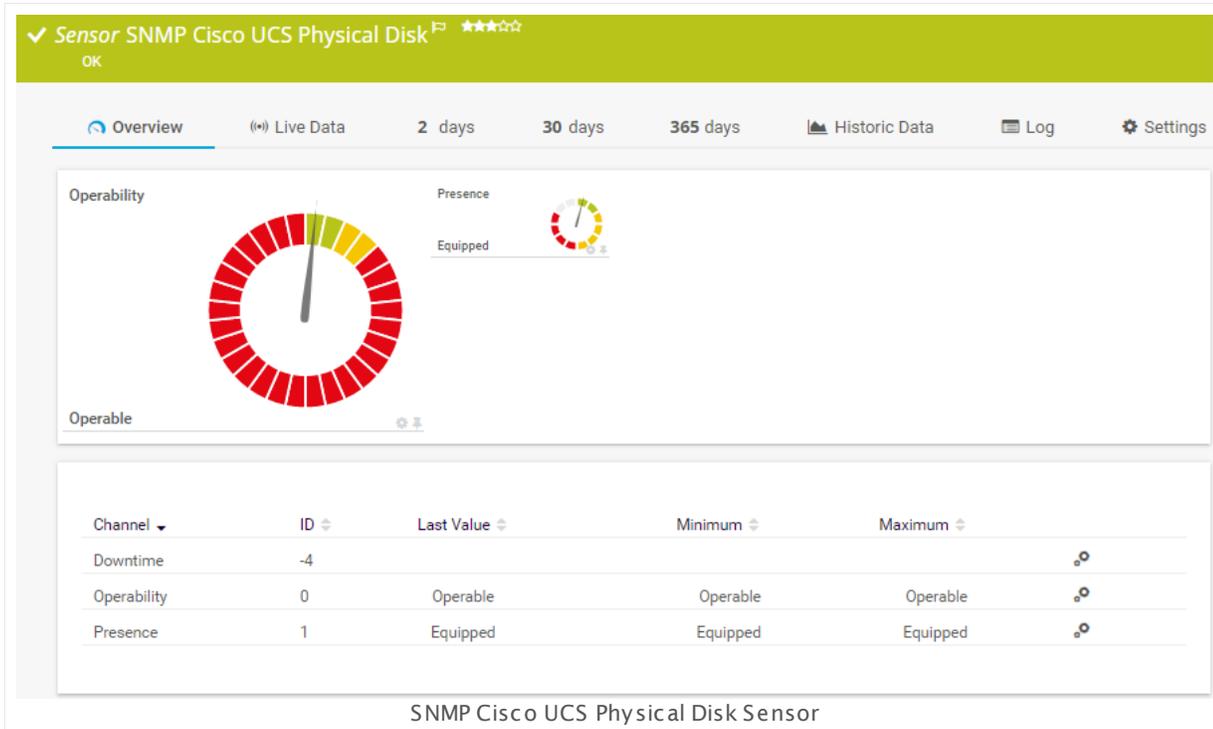
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.134 SNMP Cisco UCS Physical Disk Sensor

The SNMP Cisco UCS Physical Disk sensor monitors a physical disk of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the following:

- Operability status of the disk
- Connection status of the disk



Sensor in Other Languages

Dutch: **SNMP-Cisco UCS fysieke schijf**, French: **Disque physique UCS Cisco SNMP**, German: **SNMP Cisco UCS Physikalisches Laufwerk**, Japanese: **SNMP Cisco UCS**, Portuguese: **Disco físico de UCS Cisco de SNMP**, Russian: **Физический диск SNMP Cisco UCS**, Simplified Chinese: **SNMP Cisco UCS**, Spanish: **Disco físico Cisco UCS de SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

To monitor physical disks in a UCS device, PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

UCS PHYSICAL DISK

Disks

Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 This list only shows working disks with the current status **Up** or **Warning**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3270], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags

Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

UCS PHYSICAL DISK

Disk	<p>Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Display Name	<p>Shows the display name of the physical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p>

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

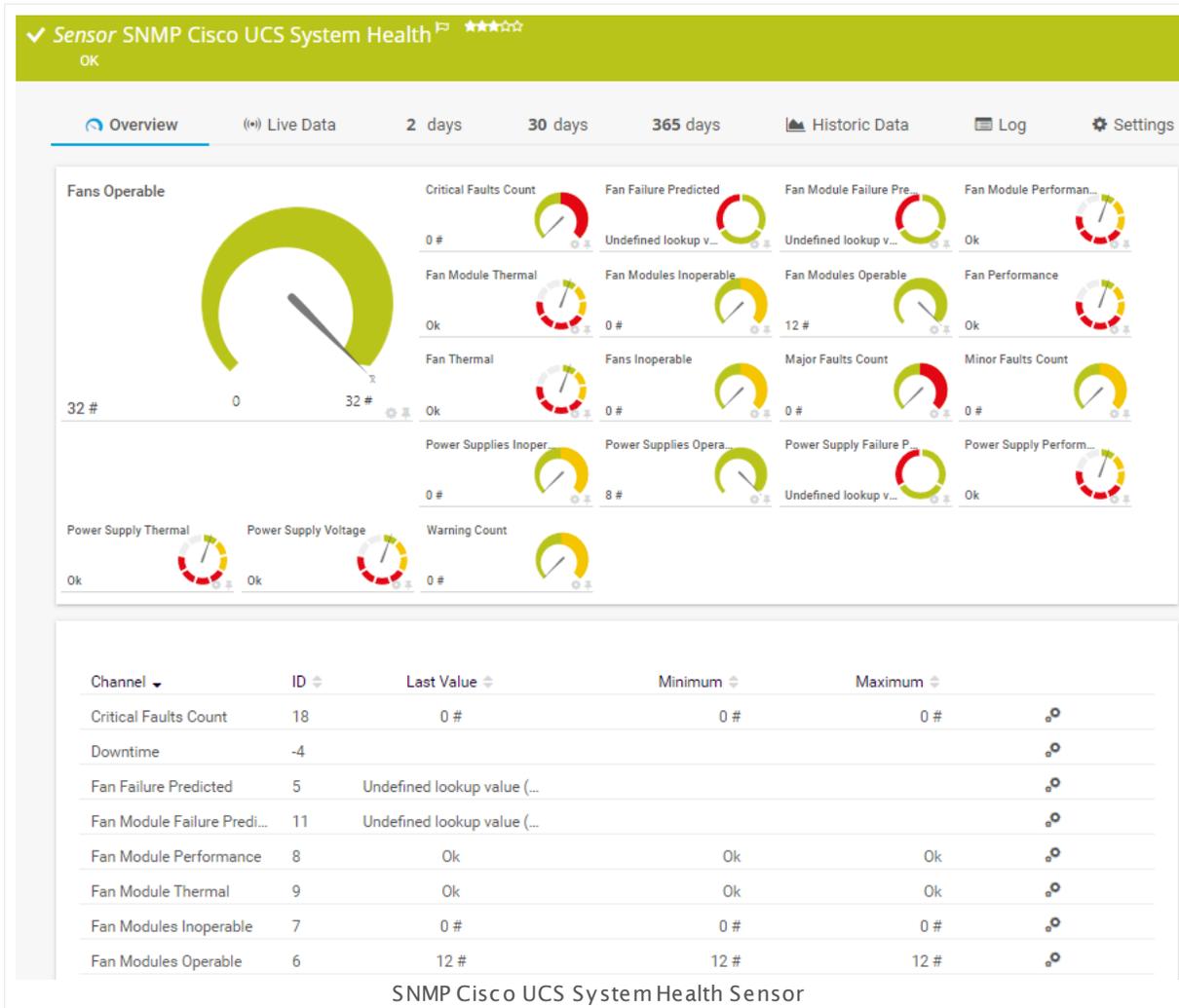
7.8.135 SNMP Cisco UCS System Health Sensor

The SNMP Cisco UCS System Health sensor monitors the system health of a Cisco Unified Computing System (UCS) device via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of operable and inoperable fans
- Status of fan performance, fan thermal, and fan voltage
- Number of operable and inoperable fan modules
- Status of fan module performance, fan module thermal, and fan module voltage
- Number of operable and inoperable power supplies
- Status of power supply performance, power supply thermal, and power supply voltage
- Number of minor, major, and critical faults (that are not yet acknowledged in the UCS logs)
- Number of warnings (that are not yet acknowledged in the UCS logs)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP Cisco UCS System Health**, French: **État du système SNMP Cisco UCS**, German: **SNMP Cisco UCS Systemzustand**, Japanese: **SNMP Cisco UCS ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema UCS SNMP Cisco**, Russian: **Работоспособность системы SNMP Cisco UCS**, Simplified Chinese: **SNMP Cisco UCS ? ? ? ? ? ? ?**, Spanish: **Estado del sistema Cisco UCS del SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#) [3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) [3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹³⁶. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

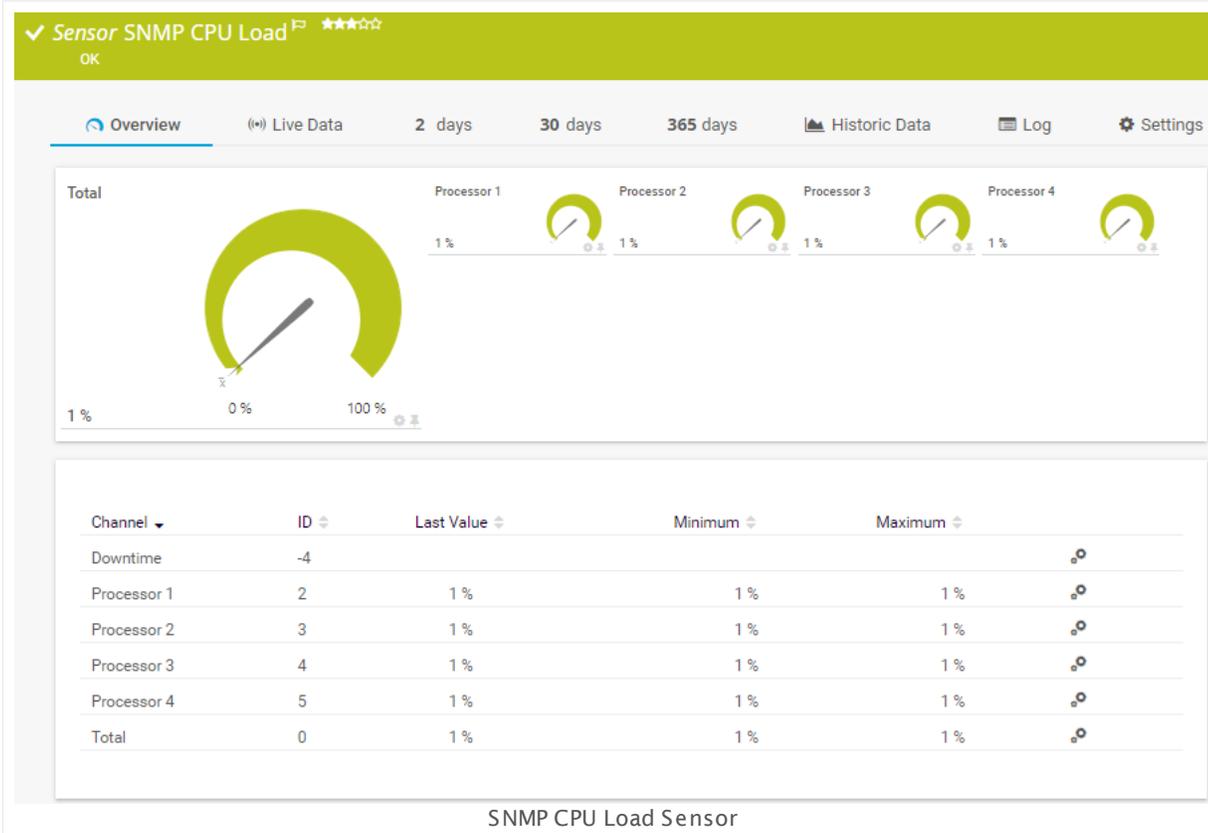
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.136 SNMP CPU Load Sensor

The SNMP CPU Load sensor monitors the system load using Simple Network Management Protocol (SNMP).

- It shows the load of several CPUs in percent.



Sensor in Other Languages

Dutch: **SNMP CPU Load**, French: **Charge CPU SNMP**, German: **SNMP Prozessorlast**, Japanese: **SNMP CPU ? ?**, Portuguese: **Carga da SNMP CPU**, Russian: **Загрузка ЦП SNMP**, Simplified Chinese: **SNMP CPU ? ?**, Spanish: **SNMP Carga de CPU**

Remarks

- It might not work to query data from a probe device via SNMP (querying **localhost**, **127.0.0.1**, or **:::1**). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

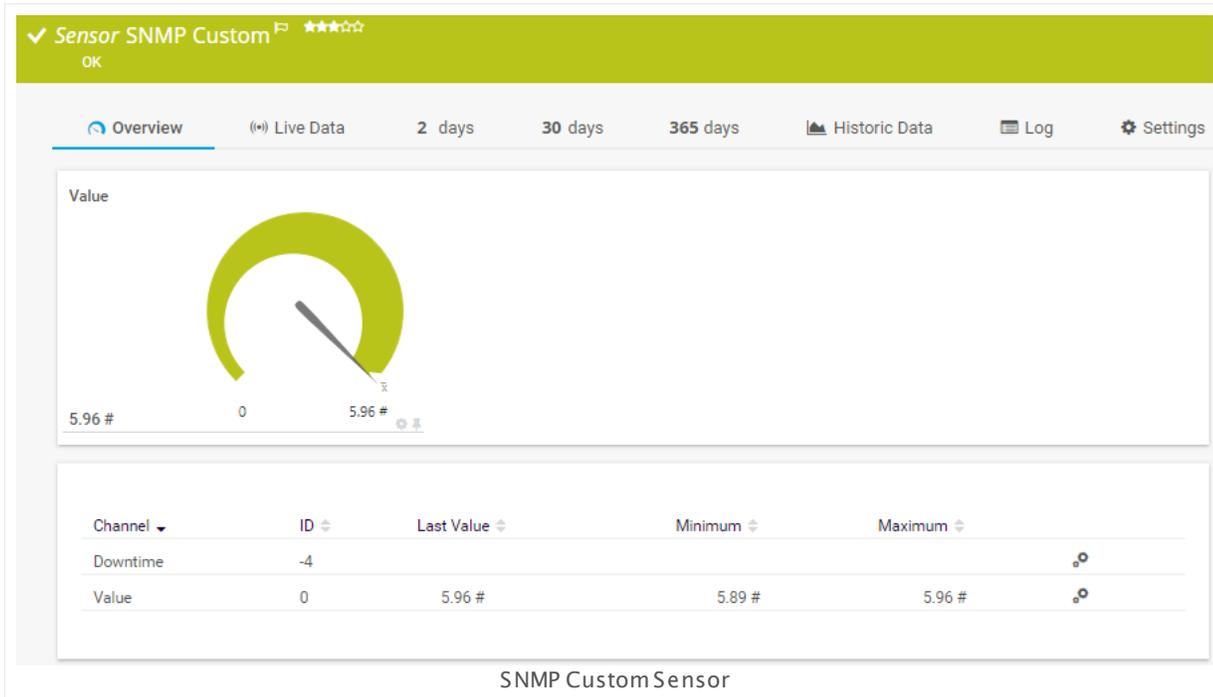
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.137 SNMP Custom Sensor

The SNMP Custom sensor monitors a single parameter that is returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP).

- This sensor shows a single numerical value (int64) for a given OID. Each OID always refers to a specific parameter of a certain SNMP device.



Sensor in Other Languages

Dutch: **SNMP (Klant specifiek)**, French: **SNMP (personnalisé)**, German: **SNMP (Benutzerdef.)**, Japanese: **SNMP ? ? ? ?**, Portuguese: **SNMP customizado**, Russian: **Пользовательские параметры SNMP**, Simplified Chinese: **SNMP ? ? ?**, Spanish: **SNMP personalizado**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do I find out what OID I need to use for a custom sensor?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Channel Name Enter a name for the channel in which the sensor shows the results for the given OID. Please enter a string. You can change this value later in the corresponding [channel settings](#)³¹⁶⁰ of this sensor.

Value Type Select the expected numeric type of the results at the given OID. Choose between:

- **Absolute (unsigned Integer):** Integer values, without an operational sign, such as **10** or **120**.
- **Absolute (signed integer):** For integer values, including an operational sign, such as **-12** or **120**.
- **Absolute (float):** For float values, such as **-5.80** or **8.23**.
- **Delta (Counter):** For counter values. PRTG will calculate the difference between the last and the current value. The delta value will additionally be divided by a time period to indicate a speed value.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Unit String Enter the unit for the values that this sensor returns. Please enter a string. This unit string is used for display purposes and will be shown in graphs, data tables, and gauges. If you want to change the **Unit** after having created the sensor, you can change it in the sensor's [channel settings](#)³¹⁶⁰.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value	<p>Enter the OID of the SNMP object you want to receive numerical data from.</p> <p>i Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string norfccheck: to the beginning of your OID, for example, norfccheck:2.0.0.0.1.</p>
-----------	--

OID VALUES

Value Type	Shows the value type of the numerical data, that this sensor receives from the given OID. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier here. Use the default value 1 to not change the received value. Please enter an integer value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Use the default value 1 to not change the received value. Please enter an integer value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>3170</small> whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor. <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor. <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings <small>3160</small> settings).</p>

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Video Tutorial: How to Set Up an SNMP Custom Sensor

- <https://www.paessler.com/support/videos/prtg-advanced/snmp-custom-and-library-sensor>

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <https://kb.paessler.com/en/topic/903>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.138 SNMP Custom Advanced Sensor

The SNMP Custom Advanced sensor monitors numerical values returned for Object Identifiers (OIDs) using Simple Network Management Protocol (SNMP).

- The sensor displays numerical values for given OIDs that refer to this specific SNMP device. Up to 10 OIDs and corresponding numerical values are possible.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

i The [SNMP Library sensor](#) will automatically create SNMP Custom Advanced sensors when the imported Management Information Base (MIB) file contains single values.

Channel	ID	Last Value	Minimum	Maximum
Battery Actual Voltage	4	55 V DC	55 V DC	55 V DC
Battery Temperature	3	27.4 °C	27.4 °C	27.4 °C
Downtime	-4			
Input Frequency	9	60 Hz	60 Hz	60 Hz
Input Line Voltage	5	127.4 V AC	127.4 V AC	127.4 V AC
Output Frequency	10	60 Hz	60 Hz	60 Hz
Output Load	7	7 %	7 %	7 %
Output Voltage	6	127.4 V AC	127.4 V AC	127.4 V AC
Run Time Remaining	2	708 d	708 d	708 d
System Uptime	8	28 d	28 d	28 d

SNMP Custom Advanced Sensor

Sensor in Other Languages

Dutch: **SNMP-geavanceerde douane**, French: **SNMP personnalisé avancé**, German: **SNMP (Benutzerdef. erweitert)**, Japanese: **SNMP ? ? ? ? ? ? ? ? ? ?**, Portuguese: **SNMP customizado avançado**, Russian: **Дополнительные пользовательские параметры SNMP**, Simplified Chinese: **SNMP ? ? ? ? ?**, Spanish: **SNMP personalizado avanzado**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do I find out what OID I need to use for a custom sensor?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Value Type

Select the expected numeric type of the results at the given OID. Choose between:

- **Absolute (unsigned Integer)**: For integer values, such as `10` or `120`.
- **Absolute (signed integer)**: For integer values, such as `-12` or `120`.
- **Absolute (float)**: For float values, such as `-5.80` or `8.23`. This value type is not compatible with the unit **Value Lookup**.
- **Delta (Counter)**: For counter values. PRTG will calculate the difference between the last and the current value. The delta value will additionally be divided by a time period to indicate a speed value. This value type is not compatible with the unit **Value Lookup**.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #2 – #10

You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for **Sensor Channel #1** without enabling it manually. Additionally you can define **Sensor Channel #2** up to **Sensor Channel #10**. To do so, choose between:

OID VALUES

- **Disable:** The sensor will not create this channel.
- **Enable:** The sensor will create this channel. Specify name, OID, value type, and unit for this channel below.

Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew. It is not possible to enable or disable sensor channels after creation of this sensor!

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) [402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) [181], as well as in [alarms](#) [219], [logs](#) [228], [notifications](#) [3216], [reports](#) [3252], [maps](#) [3276], [libraries](#) [3235], and [tickets](#) [230].

Parent Tags Shows [Tags](#) [139] that this sensor [inherits](#) [140] from its [parent device, group, and probe](#) [133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) [139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) [140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

Sensor Channel #x Name Enter a name for the channel in which the sensor shows the results at the given OID. Please enter a string.

Sensor Channel #x OID Enter the OID of the SNMP object you want to receive numerical data from.

 Most OIDs begin with **1.3.6.1**. However, entering OIDs starting with **1.0**, or **1.1**, or **1.2** is also allowed. If you want to disable the validation of your entry during your typing entirely, add the string **norfccheck:** to the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.

Sensor Channel #x Value Type Shows the value type of the numerical data that this sensor receives from the given OID. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Unit Define the unit of the numerical data that this sensor receives from the given OID. Choose between:

- BytesBandwidth
- BytesMemory
- BytesDisk
- Temperature
- Percent
- TimeResponse
- TimeSeconds
- TimeHours
- Count
- CPU
- BytesFile

OID VALUES

- SpeedDisk
- SpeedNet
- Custom
- Value Lookup

 For more information about the available units, see section [Custom Sensors](#)³⁶⁴².

 To use [lookups](#)³⁶⁹³ with this channel, choose the unit **Value Lookup** and select your lookup file below. Do not use the unit **Custom** for using lookups with this sensor and do not use the [channel settings](#)³¹⁶⁰ to define a lookup file!

 Using the unit **Value Lookup** is not possible when you choose the value type **Delta (Counter)** or **Absolute (float)**. You will not be able to create the sensor in this case.

Sensor Channel #x
Custom Unit

This setting is only available if you select the **Custom** unit option above. Define a unit for the channel value. Please enter a string.

Sensor Channel #x
Value Lookup

This setting is only available if you select the **Value Lookup** option above. Choose a [lookup](#)³⁶⁹³ file that you want to use with this channel.

Sensor Channel #y

This field shows the option you chose for this channel in the [Add Sensor](#)¹⁹⁶⁰ dialog, **Enable** or **Disable**. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

If you created this channel, you can define the settings of this channel as described above.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <https://kb.paessler.com/en/topic/903>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.139 SNMP Custom String Sensor

The SNMP Custom String sensor monitors a string returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP). It can check for keywords. If you want to set limits to the sensor channel value, you can also extract a numeric value contained in the string.

This sensor shows the following:

- Response time of the monitored device
- Optionally a value extracted from the string
- In the sensor message, the sensor shows the string you [search](#) for and which is the reason for a current **Warning** or **Down status**.

i The [SNMP Library sensor](#) will automatically create SNMP Custom String sensors when the imported Management Information Base (MIB) file contains string values.

Linux 4.4.0-59-generic #80-Ubuntu SMP Fri Aug 4 17:47:47 UTC 2017 x86_64

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Response Time 3 msec 0 10 msec

Extracted Value 0

Channel	ID	Last Value	Minimum	Maximum
Downtime	-4			
Extracted Value	2	0	0	0
Response Time	3	3 msec	1 msec	10 msec

SNMP Custom String Sensor

Sensor in Other Languages

Dutch: **SNMP Aangepaste Tekenreeks**, French: **Chaîne personnalisée SNMP**, German: **SNMP-Zeichenfolge**, Japanese: **SNMP ? ? ? ? ? ?**, Portuguese: **Sequência de caracteres customizada SNMP**, Russian: **SNMP: строка ответа**, Simplified Chinese: **SNMP ? ? ? ? ? ?**, Spanish: **Cadena personalizada de SNMP**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do I find out what OID I need to use for a custom sensor?](#)
- Example: [Number Extraction with Regular Expression](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value Enter the OID of the SNMP object you want to receive a string from.

 Most OIDs begin with **1.3.6.1**. However, entering OIDs starting with **1.0**, or **1.1**, or **1.2** is also allowed. If you want to disable the validation of your entry entirely, add the string **norfccheck:** at the beginning of your OID, for example, **norfccheck:2.0.0.0.1**.

Maximum Length of String Define the maximum allowed length of the string to be received from the SNMP object at the given OID. If the string is longer than this value, the sensor shows a **Down status**^[195]. Please enter an integer value or leave the field empty.

If Value Changes Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)^[3170] whenever the sensor value changes.

KEYWORD SEARCH

Response Must Include (Error State) Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a [Regular Expression](#)^[3704]. If the data does not include the search pattern, the sensor shows a **Down status**^[195]. Please enter a string or leave the field empty.

For Keyword Search Use Define in which format you have entered the search expression in the field above.

- **Plain Text:** Search for the string as plain text. The characters asterisk `*` and question mark `?` work here as placeholder, whereas `*` stands for no or any number of characters and `?` stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search.
- **Regular Expression:** Use the search pattern as a [Regular Expression](#)^[3704].

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

Response Must Not Include (Error State) Define which string must **not** be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a [Regular Expression](#)^[3704]. If the data does include the search pattern, the sensor shows a **Down status**^[195]. Please enter a string or leave the field empty.

For Keyword Search Use Define in which format you have entered the search expression in the field above.

- **Plain Text:** Search for the string as plain text. The characters asterisk `*` and question mark `?` work here as placeholder, whereas `*` stands for no or any number of characters and `?` stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search.
- **Regular Expression:** Use the search pattern as a [Regular Expression](#)^[3704].

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

KEYWORD SEARCH

Response Must Include (Warning State)	Define which string must be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a Regular Expression ^[3704] . If the data does not include the search pattern, the sensor shows a Warning status ^[195] . Please enter a string or leave the field empty.
For Keyword Search Use	<p>Define in which format you have entered the search expression in the field above.</p> <ul style="list-style-type: none"> ▪ Plain Text: Search for the string as plain text. The characters asterisk <code>*</code> and question mark <code>?</code> work here as placeholder, whereas <code>*</code> stands for no or any number of characters and <code>?</code> stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Use the search pattern as a Regular Expression^[3704]. <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions^[3704].</p>
Response Must Not Include (Warning State)	Define which string must not be part of the data that is received from the SNMP object at the given OID. You can either enter plain text or a Regular Expression ^[3704] . If the data does include the search pattern, the sensor shows a Warning status ^[195] . Please enter a string or leave the field empty.
For Keyword Search Use	<p>Define in which format you have entered the search expression in the field above.</p> <ul style="list-style-type: none"> ▪ Plain Text: Search for the string as plain text. The characters asterisk <code>*</code> and question mark <code>?</code> work here as placeholder, whereas <code>*</code> stands for no or any number of characters and <code>?</code> stands for exactly one character (as known from Windows search). You cannot disable this behavior, so the literal search for these characters is not possible with plain text search. ▪ Regular Expression: Use the search pattern as a Regular Expression^[3704]. <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions^[3704].</p>

EXTENDED PROCESSING

Interpret Result as	<p>Define the type of the received string. Choose between:</p> <ul style="list-style-type: none"> ▪ String (default): Handle the result as common string. ▪ Hexadecimal bytes (as in MAC addresses): Handle the result as hexadecimal bytes. For example, choose this option when monitoring MAC addresses. ▪ Decimal bytes (as in IP addresses): Handle the result as decimal bytes. For example, choose this option when monitoring IP addresses.
Extract Number Using Regular Expression	<p>Define if you want to filter out a numeric value from the string received from the SNMP object at the given OID. You can convert this into a float value to use it with channel limits (see Sensor Channels Settings³¹⁶⁰).</p> <ul style="list-style-type: none"> ▪ No extraction: Do not extract a float value. Use the result as a string value. ▪ Extract a numeric value using a regular expression: Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below. See also the example¹⁹⁸⁰ below.
Regular Expression	<p>This setting is only visible if you enable number extraction above. Enter a Regular Expression³⁷⁰⁴ to identify the numeric value you want to extract from the string returned by the SNMP object at the given OID. You can use capturing groups here.</p> <p>Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.</p> <p> PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section Regular Expressions³⁷⁰⁴.</p>
Index of Capturing Group	<p>This setting is only visible if you enable number extraction above. If your regular expression uses capturing groups, please specify which one will be used to capture the number. Please enter an integer value or leave the field empty.</p>
Decimal Separator	<p>This setting is only visible if you enable number extraction above. Define which character is used as decimal separator for the number extracted above. Please enter a string or leave the field empty.</p>

EXTENDED PROCESSING

Thousands Separator This setting is only visible if you enable number extraction above. Define which character is used as thousands separator for the number extracted above. Please enter a string or leave the field empty.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- User Group Access** Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:
- **Inherited:** Use the access rights settings of the parent object.
 - **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
 - **Read:** Users in this group can see the object and review its monitoring results.
 - **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
 - **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Example: Number Extraction with Regular Expression

 If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on **1 (not on 0)**. Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number **3.555**, that is the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As **Index of Capturing Group** enter **3**. This will extract the desired number **3.555**.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains 3.49%, 1 Min (3.555), 5 Min (3.90)
- Group 2 contains 3.49
- Group 3 contains 3.555
- Group 4 contains 3.90

Please keep in mind this note about index and capturing groups when using number extraction.

 It is not possible to match an empty string with the PRTG regex sensor search.

 PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)³⁷⁰⁴.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <https://kb.paessler.com/en/topic/903>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

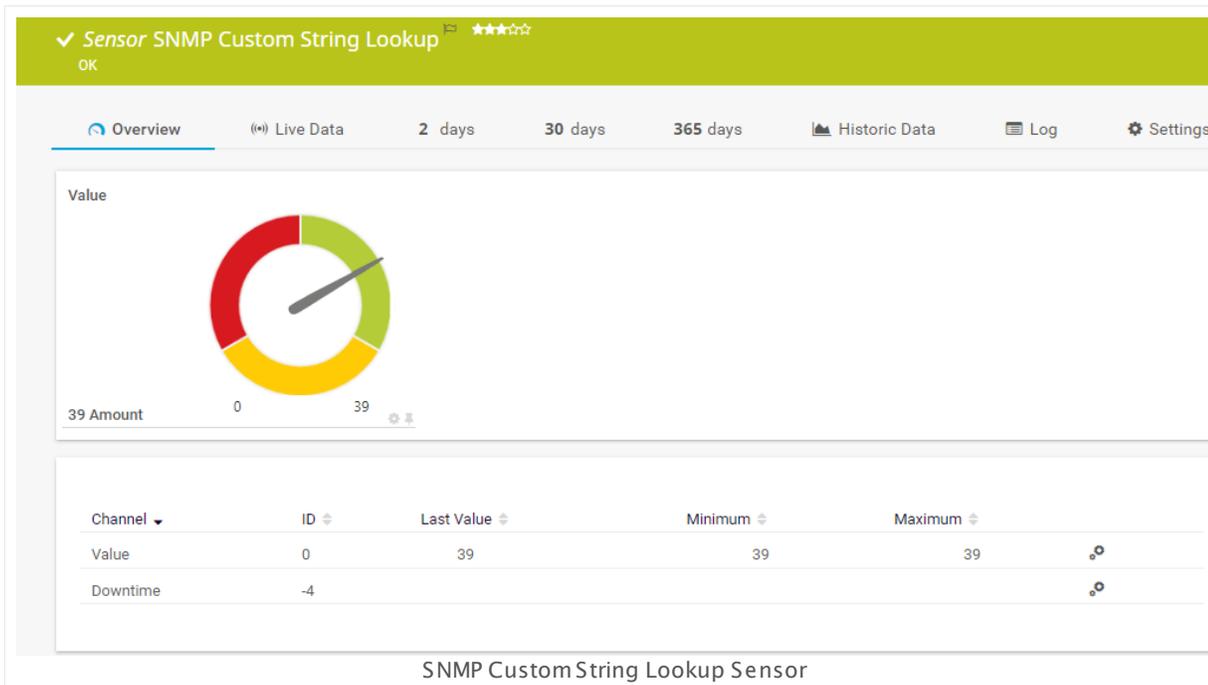
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.140 SNMP Custom String Lookup Sensor

The SNMP Custom String Lookup sensor monitors a string that a specific Object Identifier (OID) returns via Simple Network Management Protocol (SNMP). It can map the string directly to a [sensor status](#)^[195] by using a [defined lookup file](#)^[365]. Basically, this sensor type does a "reverse lookup". You have to define all potential return strings in the lookup file as text values, each in one lookup entry. Graphs and data tables show the value to which the string is mapped, usually an integer ([lookup type](#)^[370] **SingleInt**). See manual section [SNMP Custom String Lookup Sensor—Example](#)^[199].

- This sensor shows a retrieved string value and its status, as defined in the corresponding lookup file.



Sensor in Other Languages

Dutch: **SNMP Aangepaste Tekst Lookup**, French: **Requête de chaîne personnalisée SNMP**, German: **SNMP-Zeichenfolge mit Lookup**, Japanese: **SNMP ? ? ? ? ? ? ? ?**, Portuguese: **Pesquisa da sequência de caracteres customizada SNMP**, Russian: **Подстановка пользовательской строки по SNMP**, Simplified Chinese: **SNMP ? ? ? ? ? ? ? ?**, Spanish: **Búsqueda de cadena personalizada de SNMP**

Remarks

- See manual section [SNMP Custom String Lookup Sensor—Example](#)^[199] for a sample lookup definition for this sensor type.
- It might not work to query data from a probe device via SNMP (querying **localhost**, **127.0.0.1**, or **:::1**). [Add this device to PRTG](#)^[311] with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do I find out what OID I need to use for a custom sensor?](#)

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).
- Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

OID VALUES

Channel Name	Enter a name for the channel in which the sensor shows the results at the given OID. Please enter a string. You can change this value later in the respective channel settings of this sensor.
Lookup	Select a lookup file that you stored in the <code>\lookups\custom</code> subfolder of your PRTG installation. This lookup file must contain all potential strings that the monitored OID can return.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

OID VALUES

OID Value	<p>Enter the OID of the SNMP object you want to receive a string from.</p> <p>i Most OIDs begin with 1.3.6.1. However, entering OIDs starting with 1.0, or 1.1, or 1.2 is also allowed. If you want to disable the validation of your entry entirely, add the string norfccheck: at the beginning of your OID, for example, norfccheck:2.0.0.0.1.</p>
Lookup	Shows the lookup file that this sensor uses. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between:

OID VALUES

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³¹⁷⁰ whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[331]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Example

 You have to provide all possible return strings for this sensor in one lookup file. For example, consider an OID that can return one of the three strings **Good**, **Deficient**, or **Bad**. Then you have to [define a lookup file](#)³⁰⁹³ for this sensor that contains all these possible string values as text, each text value in one lookup entry:

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

140 SNMP Custom String Lookup Sensor

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="mylookupfile" desiredValue="0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:
  <Lookups>
    <SingleInt state="Ok" value="0">
      Good
    </SingleInt>
    <SingleInt state="Warning" value="1">
      Deficient
    </SingleInt>
    <SingleInt state="Error" value="2">
      Bad
    </SingleInt>
  </Lookups>
</ValueLookup>
```

If a retrieved string matches one of the text values, the sensor maps it into the defined integer value ("reverse lookup") that is shown, for example, in data graphs. Depending on the integer, the sensor shows the according status and converts the integer back to the original string to show it as channel value. If the OID returns a string that the lookup definition does not contain, the sensor will show a **Down status** with a corresponding error message.

For example, you create an SNMP Custom String Lookup sensor, apply the example lookup definition from above (store it into the `\lookups\custom` subfolder of your PRTG installation), and the given OID returns the string **Good**. Then the sensor maps **Good** into the integer value **0**, shown in the live graph of the sensor, for example. According to the status definition `state="Ok"`, the **sensor status** is **Up** in this case. The integer **0** is converted back to the string **Good**, which is shown as channel value.

 The string match is not case sensitive.

 Use the lookup type **SingleInt** for this sensor. BitFields and ranges are not supported!

 If you [imported an SNMP library](#) (this is an `oidlib` file) that contains [lookups](#) (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. Use the **lookupname** of the imported SNMP library as **id** parameter in a custom lookup definition. This overrides the lookups that an `oidlib` might contain with your own status definitions. See section [Define Lookups—Customizing Lookups](#) for details about this mechanism.

More

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <https://kb.paessler.com/en/topic/903>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

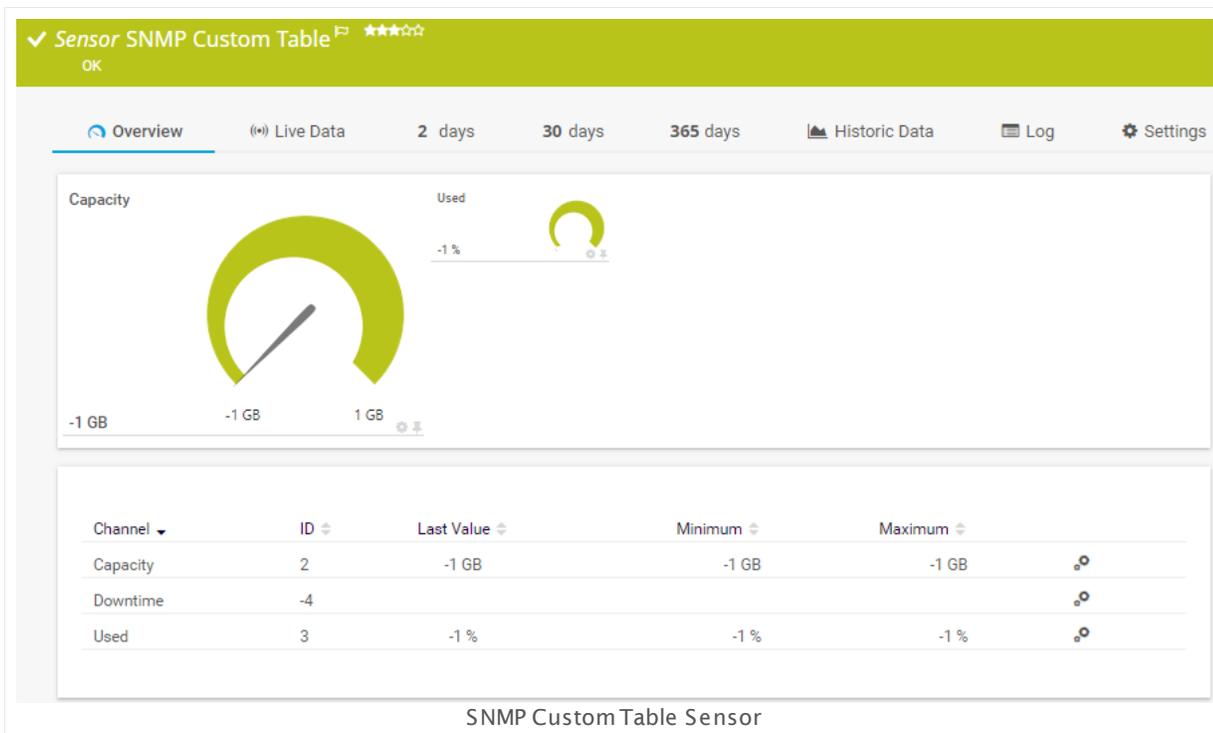
7.8.141 SNMP Custom Table Sensor

The SNMP Custom Table sensor monitors entries from a table that is provided via Simple Network Management Protocol (SNMP). You can create one new sensor per table row. For each sensor, you can define up to ten channels. Each channel shows the value of one defined table column.

- It can show numerical values in up to 10 channels per table row.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

i The [SNMP Library sensor](#)²²³⁷ will automatically create SNMP Custom Table sensors when the imported Management Information Base (MIB) file contains tables.



Sensor in Other Languages

Dutch: **SNMP Aangepaste Tabel**, French: **Table SNMP personnalisée**, German: **SNMP (Benutzerdef. Tabelle)**, Japanese: **SNMP ? ? ? ? ? ? ? ?**, Portuguese: **Tabela customizada do SNMP**, Russian: **Нестандартная таблица SNMP**, Simplified Chinese: **SNMP ? ? ? ?**, Spanish: **Tabla de SNMP personalizado**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#)³¹¹ with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do I find out what OID I need to use for a custom sensor?](#)

- Knowledge Base: [What can I monitor with the SNMP Custom Table Sensor?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

PRTG will create one SNMP Table sensor for each table row that you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP TABLE

Table OID Enter the OID of the SNMP table you want to monitor. The OID needs to point directly to an object that represents an SNMP table. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

 Without entering an OID, you cannot proceed to the sensor and sensor channel creation.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. You can use the placeholders **[tablename]** and **[rowidentifier]**. They will be replaced with the name of the table and the identifying value of the chosen row respectively. You can choose the column that provides the row identifier in the **Identification Column** option below.

You can also enter a valid OID that is part of a different SNMP table, for example, **[1.3.6.1.2.1.2.1.2]**, to query information that is not contained in the current table. The same index as in the original table will be added to the OID.

TABLE SPECIFIC

Table

Choose the relevant table rows in which you find the data that you want to monitor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

PRTG shows you the table that the OID you entered before returns. To better find what you want to monitor, especially in large tables, use the search function in the upper right corner.

Identification Column

Define the identification column for the SNMP Table sensor(s) you want to create. The sensor uses this column to uniquely identify each table row. This column should preferably be unique because it will allow the sensor to keep track of changing indexes.

The value of the column that you choose as the identification column will replace the **[row identifier]** in the sensor name. This allows you to distinguish sensors that are created for the same SNMP table.

 One new sensor is created for each table row you choose.

Sensor Channel #2 - #10

You can create up to 10 different sensor channels for this sensor. You have to define at least one data channel, so you will see all available settings for **Sensor Channel #1** without enabling it manually. Additionally you can define **Sensor Channel #2** up to **Sensor Channel #10**. To do so, choose between:

- **Disable:** The sensor will not create this channel.
- **Enable:** Create an additional channel and define all its characteristics below, its name, column, value type, and unit.

It is not possible to enable or disable sensor channels after the creation of this sensor!

 All sensor channels that you define while creating an SNMP Table sensor will be the same for all sensors for each table row.

Value Type

Select the expected type of the results in this channel. Choose between:

- **Absolute (unsigned Integer):** For integer values, such as **10** or **120**.
- **Absolute (signed integer):** For integer values, such as **-12** or **120**.

TABLE SPECIFIC

- **Absolute (float):** For float values, such as **-5.80** or **8.23**. This value type is not compatible with the unit **Value Lookup**.
- **Delta (Counter):** For counter values. PRTG will calculate the difference between the last and the current value. The delta value will additionally be divided by a time period to indicate a speed value. This value type is not compatible with the unit **Value Lookup**.

See [below](#) for the other channel settings that can be changed also after the sensor has been created.

i This sensor monitors numerical values only. Make sure that you do not select columns that return strings because they lead to a **Down status**. For example, if you monitor an **ifTable**, we recommend that you do not select an **ifDescr** column because this will result in an error.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP TABLE

Table OID Shows the OID of the SNMP table that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

TABLE SPECIFIC

Identifier This is the value of the column that you selected as the **Identification Column** during the sensor creation. It is also displayed in the sensor name to distinguish it from other sensors you created for the same table with other table rows. You can change the identifier if you want to.

Identification Column Shows the table column that you chose as the identification column. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Sensor Channel #x Name Enter a name for the channel in which the sensor shows the desired result. Please enter a string.

Sensor Channel #x Column Select the table column that together with the table row points to the value that you want to monitor in this channel. You can choose between the available columns of the table that you monitor.

TABLE SPECIFIC

Sensor Channel #x Value Type	Shows the value type of the data that this sensor receives in this channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Channel #x Unit	<p>Define the unit of the data that this sensor receives in this channel. Choose between:</p> <ul style="list-style-type: none"> ▪ BytesBandwidth ▪ BytesMemory ▪ BytesDisk ▪ Temperature ▪ Percent ▪ TimeResponse ▪ TimeSeconds ▪ TimeHours ▪ Count ▪ CPU ▪ BytesFile ▪ SpeedDisk ▪ SpeedNet ▪ Custom ▪ Value Lookup <p> For more information about the available units, see section Custom Sensors³⁶⁴².</p> <p> To use lookups³⁶⁹³ with this channel, choose the unit Value Lookup and select your lookup file below. Do not use the unit Custom for using lookups with this sensor and do not use the channel settings³¹⁶⁰ to define a lookup file!</p> <p> Using the unit Value Lookup is not possible when you choose the value type Delta (Counter) or Absolute (float). You will not be able to create the sensor in this case.</p>
Sensor Channel #x Custom Unit	This setting is only visible if you select the Custom unit option above. Define a unit for the channel value. Please enter a string.

TABLE SPECIFIC

Sensor Channel # x Value Lookup	This setting is only visible if you select the Value Lookup option above. Select a lookup <small>3683</small> file that you want to use with this channel.
Sensor Channel # x+1	Shows if you enabled or disabled a channel. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings <small>3160</small> settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) 331 group's settings, see section [Inheritance of Settings](#) 137 for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- ❗ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: What can I monitor with the SNMP Custom Table Sensor?

- <https://kb.paessler.com/en/topic/68539>

Knowledge Base: How to monitor a no-break (UPS) device complying to the UPS-MIB (RFC 1628)

- <https://kb.paessler.com/en/topic/72117>

Knowledge Base: How do I find out what OID I need to use for a custom sensor?

- <https://kb.paessler.com/en/topic/903>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

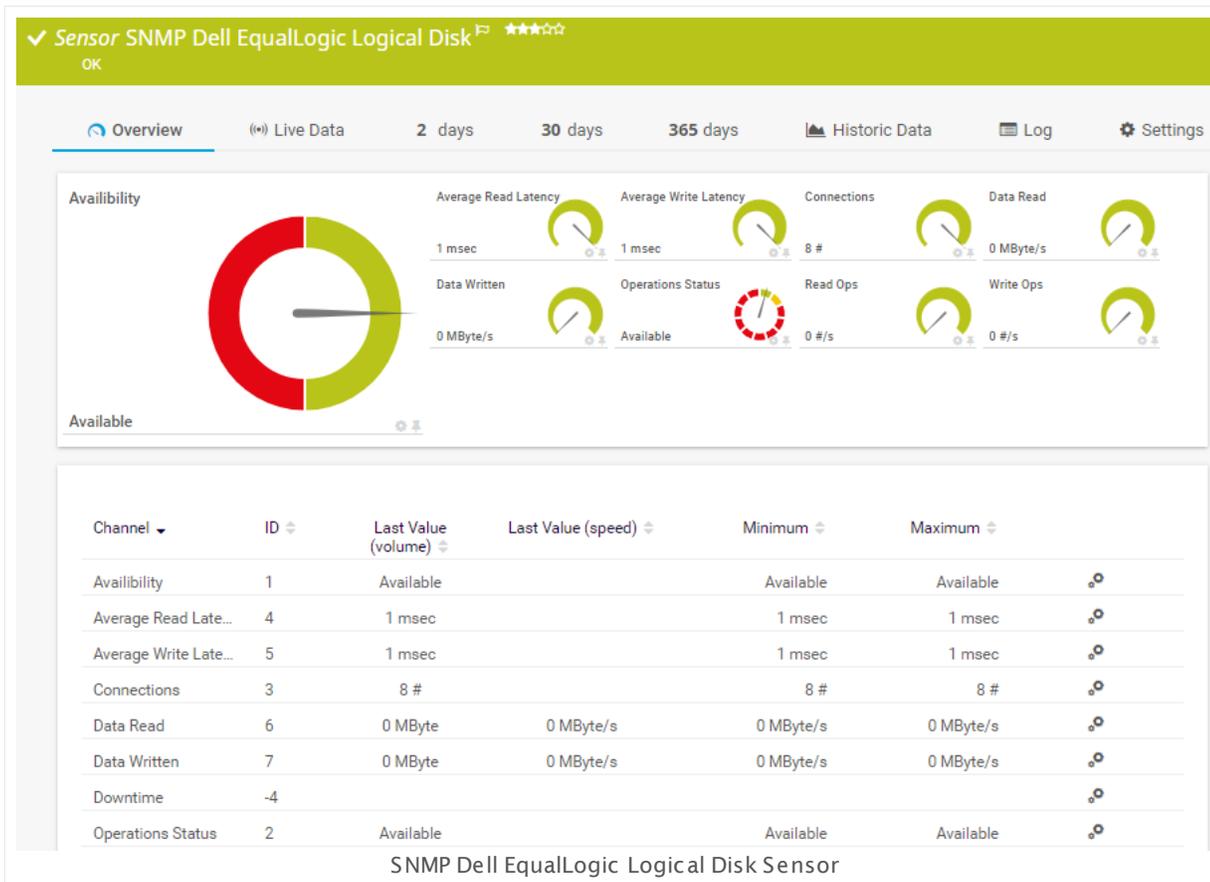
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.142 SNMP Dell EqualLogic Logical Disk Sensor

The SNMP Dell EqualLogic Logical Disk sensor monitors a volume of a Dell EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Availability
- Average read/write latency
- Number of connections
- Amount of read/written data
- Operational status
- Number of IOPS (Input/Output operations per second)



Sensor in Other Languages

Dutch: **SNMP Dell EqualLogic Logische Schijf**, French: **Disque logique Dell EqualLogic SNMP**, German: **SNMP Dell EqualLogic Logischer Datenträger**, Japanese: **SNMP Dell Equal Logic c? ? ? ? ?**, Portuguese: **Disco lógico SNMP Dell EqualLogic**, Russian: **Логический диск SNMP Dell EqualLogic**, Simplified Chinese: **SNMP Dell EqualLogic ? ? ? ?**, Spanish: **Disco lógico SNMP de Dell EqualLogic**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volume(s) from the storage system that you want to monitor. PRTG will create one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Volume	Select the volume(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Volume	Shows the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the identifier of the array member. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Volume ID	Shows the ID of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DELL EQUALLOGIC SPECIFIC

Volume Description Shows the description of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.143 SNMP Dell EqualLogic Member Health Sensor

The SNMP Dell EqualLogic Member Health sensor monitors the health of an array member of an EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Member status
- Cooling power of the fan module in rpm (rotations per minute)
- Power supply status of cooling system
- Temperature of the backplane
- Temperature measured by temperature control module
- System temperature
- Member health status
- RAID status
- Average read/write latency in milliseconds or as percentage of the largest value
- Free storage capacity
- Amount of data handled per second
- Number of spare drives available

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 143 SNMP Dell EqualLogic Member Health Sensor



Sensor in Other Languages

Dutch: **SNMP Dell EqualLogic Lid Gezondheid**, French: **État du membre Dell EqualLogic SNMP**, German: **SNMP Dell EqualLogic Member-Zustand**, Japanese: **SNMP Dell EqualLogic** ? ? ? ? ? ? ? , Portuguese: **Funcionamento do membro SNMP Dell EqualLogic**, Russian: **Работоспособность элемента Dell EqualLogic по SNMP**, Simplified Chinese: **SNMP Dell EqualLogic** ? ? ? ? ? ? ? , Spanish: **Salud de miembro SNMP de Dell EqualLogic**

Remarks

- This sensor type works with **SNMP v2c** and **SNMP v3**. It does not support **SNMP v1**. Ensure you set the correct **SNMP Version** in the **Credentials for SNMP Devices** settings of the parent device or inherit it from objects higher in the [hierarchy](#)¹³³.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) on the drive you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Array Member

Select the array member(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Array Member	Shows the name of the member this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Group ID	Shows the group ID of the disk that this sensor monitors.. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the group member ID of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

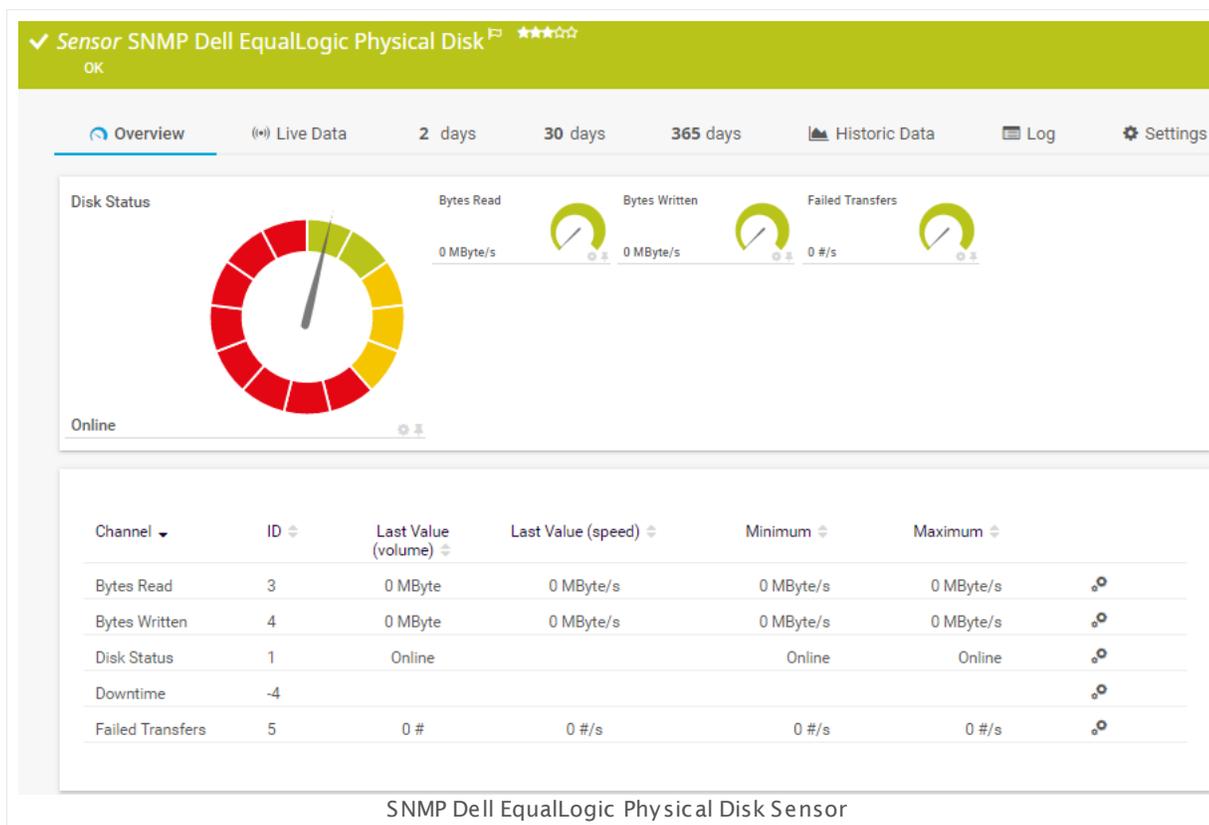
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.144 SNMP Dell EqualLogic Physical Disk Sensor

The SNMP Dell EqualLogic Physical Disk sensor monitors a disk in a Dell EqualLogic storage system via Simple Network Management Protocol (SNMP).

The sensor provides the following information:

- Disk status
- Bytes read/written
- Failed transfers
- Health status of disk



Sensor in Other Languages

Dutch: **SNMP Dell EqualLogic Fysieke Schijf**, French: **Disque physique Dell EqualLogic SNMP**, German: **SNMP Dell EqualLogic Physikalischer Datenträger**, Japanese: **SNMP Dell EqualLogic ? ? ? ? ?**, Portuguese: **Disco físico SNMP Dell EqualLogic**, Russian: **Физический диск Dell EqualLogic по SNMP**, Simplified Chinese: **SNMP Dell EqualLogic ? ? ? ?**, Spanish: **Disco físico SNMP de Dell EqualLogic**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the array member(s) of the Dell EqualLogic storage system you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL EQUALLOGIC SPECIFIC

Disk	Select the disk(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL EQUALLOGIC SPECIFIC

Disk	Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Group ID	Shows the group ID of the disk that this sensor monitors.. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Member ID	Shows the group member ID of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DELL EQUALLOGIC SPECIFIC

Disk Slot	Shows the slot number of disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Serial Number	Shows the serial number of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Manufactured	Shows the production date of the disk that this sensor monitors. If this field is empty, the disk does not provide information about the date (this depends on the manufacturer). Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.145 SNMP Dell Hardware Sensor

The SNMP Dell Hardware sensor monitors performance counters on a Dell hardware device using Simple Network Management Protocol (SNMP). The data that you can monitor with this sensor depends on the available performance counters on the target system.

This sensor shows a value returned by a specific Dell hardware OID, for example:

- Data about the system management software
- Data about system status
- Information about chassis and BIOS
- Various hardware parameters
- Other valuable data

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

i The SNMP Dell Hardware sensor will not appear as running sensor, instead it will be created as [SNMP Custom Advanced](#) ¹⁹⁵⁹ or [SNMP Custom Table sensor](#) ¹⁹⁹².

The screenshot shows the PRTG Network Monitor interface for the 'Sensor SNMP Dell Hardware'. The top bar is green and shows a checkmark, the sensor name, and a status of 'OK'. Below this are navigation tabs: 'Overview' (selected), 'Live Data', '2 days', '30 days', '365 days', 'Historic Data', 'Log', and 'Settings'. The main content area displays a gauge for 'system state global system status' with a needle pointing to 0 on a scale from 0 to 4. Below the gauge is a table with the following data:

Channel	ID	Last Value	Minimum	Maximum
Downtime	-4			
system state global sys...	0	4 #	4 #	4 #

At the bottom of the interface, the text 'SNMP Dell Hardware Sensor' is displayed.

Sensor in Other Languages

Dutch: **SNMP Dell Hardware**, French: **Matériels SNMP Dell**, German: **SNMP Dell Hardware**, Japanese: **SNMP DELL ? ? ? ? ? ?**, Portuguese: **Hardware Dell SNMP**, Russian: **Оборудование Dell по SNMP**, Simplified Chinese: **SNMP DELL ? ?**, Spanish: **Hardware SNMP Dell**

Remarks

- [Requires](#)²⁰³³ the Dell OpenManage Server Administrator to be installed on the monitored Dell device.
- Knowledge Base: [What do I need to monitor Dell servers?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: Dell OpenManage Server Administrator

 This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell hardware device to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator.

 For details, see the Knowledge Base: [What do I need to monitor Dell servers?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Dell performance counters you want to monitor. PRTG will create one [SNMP Custom Advanced](#)¹⁹⁵⁹ or [SNMP Custom Table sensor](#)¹⁹⁹² with up to 10 channels for each Library OID category you choose in the **Add Sensor** dialog. If your selection results in more than 10 channels, PRTG will create the corresponding amount of SNMP Custom Advanced or SNMP Custom Table sensors. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL HARDWARE SPECIFIC

Library OIDs

Select the performance counters you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 Choose the counters that you want to monitor with caution! We recommend that you select only a few counters in this dialog. Use the search function in the table head to filter for specific counters. Selecting too many library OIDs might result in thousands of sensors or in an aborted sensor creation.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL HARDWARE SPECIFIC

Selected Interface	Shows the name of the interface (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit String	Define the unit of the numerical data that the sensor receives at the given OID. Please enter a string.
Multiplication	If you want to multiply the received data with a certain value, enter the multiplier here. Please enter an integer value.
Division	If you want to divide the received data by a certain value, enter the divisor here. Please enter an integer value.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: <ul style="list-style-type: none">▪ Ignore changes (default): The sensor takes no action on change.▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>3170</small> whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.
Graph Type	Define how different channels will be shown for this sensor. <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- ❗ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- ❗ If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

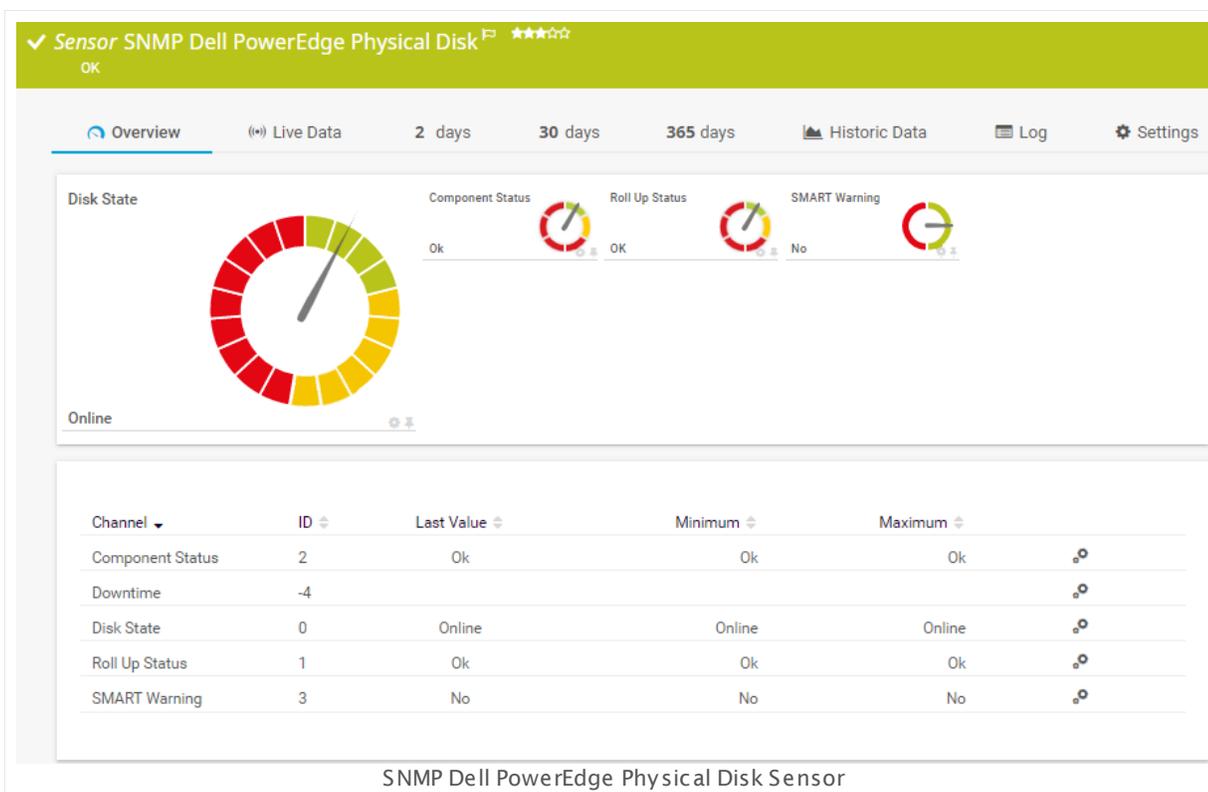
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.146 SNMP Dell PowerEdge Physical Disk Sensor

The SNMP Dell PowerEdge Physical Disk sensor monitors a physical disk in a Dell PowerEdge server using Simple Network Management Protocol (SNMP).

It can show the following:

- Disk status
- Roll up status
- Component status
- If there is currently a warning regarding the Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status



Sensor in Other Languages

Dutch: **SNMP-Dell PowerEdge Fysieke Schijf**, French: **Disque physique Dell PowerEdge SNMP**, German: **SNMP Dell PowerEdge Physikalischer Datenträger**, Japanese: **SNMP Dell PowerEdge ? ? ? ? ? ?**, Portuguese: **Disco físico SNMP Dell PowerEdge**, Russian: **Физический диск Dell PowerEdge по SNMP**, Simplified Chinese: **SNMP Dell PowerEdge ? ? ? ?**, Spanish: **Disco físico SNMP Dell PowerEdge**

Remarks

- [Requires](#) ²⁰⁵⁴ iDRAC 7 or the Dell OpenManage Server Administrator to be installed on the monitored server.

- Knowledge Base: [What do I need to monitor Dell servers?](#)
- Knowledge Base: [I can't add Dell PowerEdge sensors to PRTG. What can I do?](#)
- Knowledge Base: [Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?](#)
- Knowledge Base: [My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Requirement: Dell OpenManage Server Administrator or iDRAC 7

 This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell PowerEdge server to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator.

 For details, see the Knowledge Base: [What do I need to monitor Dell servers?](#)

 You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL POWEREDGE PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL POWEREDGE PHYSICAL DISK SETTINGS

Disk	Shows the name of the disk that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface that is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- ❗ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?

- <https://kb.paessler.com/en/topic/68040>

Knowledge Base: My Dell PowerEdge sensor fails to validate disks and I can't add it. What can I do?

- <https://kb.paessler.com/en/topic/61784>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

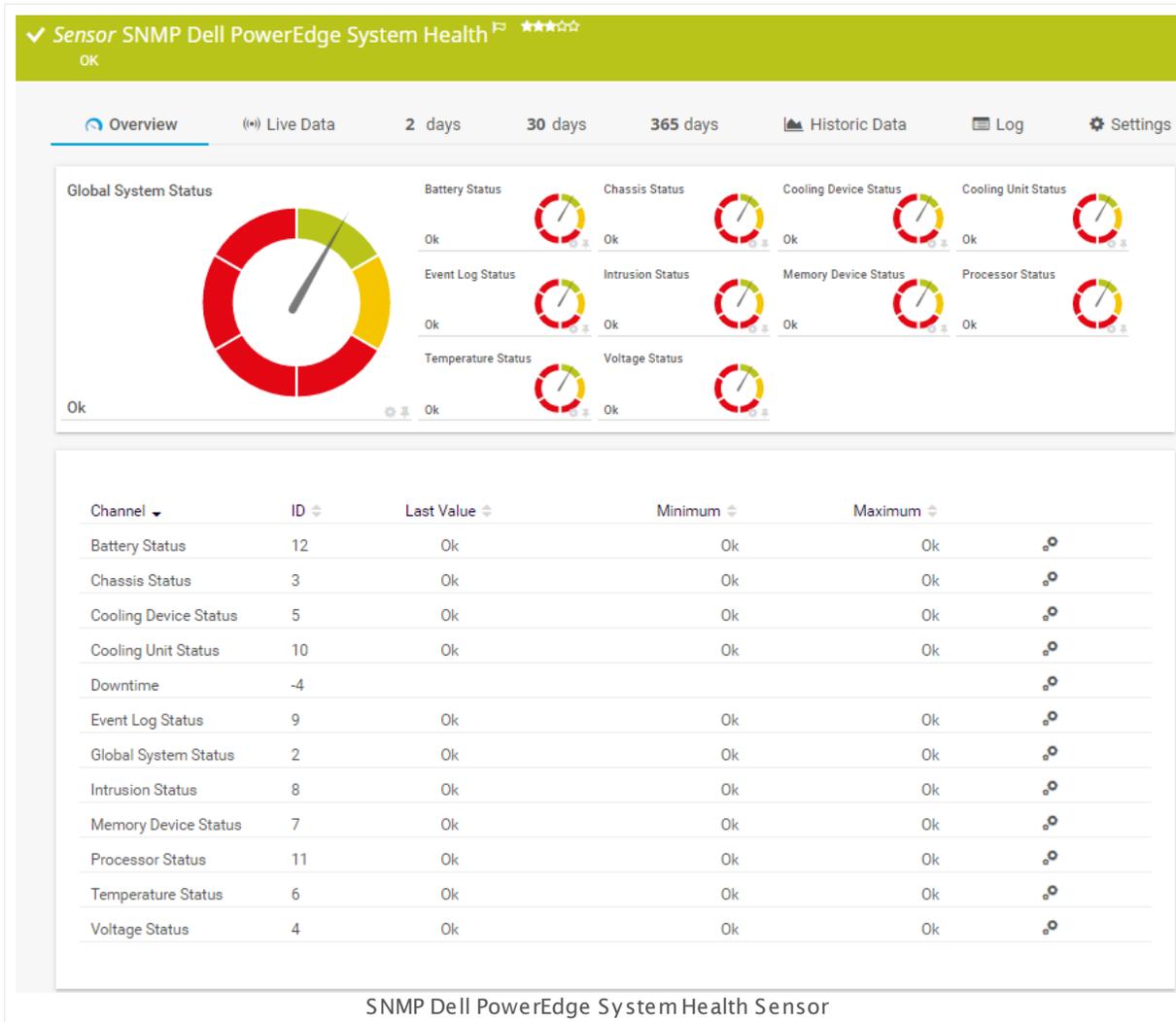
7.8.147 SNMP Dell PowerEdge System Health Sensor

The SNMP Dell PowerEdge System Health sensor monitors the system health of a Dell PowerEdge server using Simple Network Management Protocol (SNMP).

It can show the states of the following components, depending on their availability:

- Global system
- Power supply
- Temperature
- Cooling device
- Memory device
- Voltage

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP Dell PowerEdge System Status**, French: **État du système Dell PowerEdge SNMP**, German: **SNMP Dell PowerEdge Systemzustand**, Japanese: **SNMP Dell PowerEdge ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema SNMP Dell PowerEdge**, Russian: **Работоспособность системы Dell PowerEdge по SNMP**, Simplified Chinese: **SNMP Dell PowerEdge ? ? ? ? ? ?**, Spanish: **SNMP Salud de sistema Dell PowerEdge**

Remarks

- [Requires](#) ²⁰⁵⁴ iDRAC 7 or the Dell OpenManage Server Administrator to be installed on the monitored server.
- Knowledge Base: [What do I need to monitor Dell servers?](#)
- Knowledge Base: [I can't add Dell PowerEdge sensors to PRTG. What can I do?](#)
- Knowledge Base: [Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?](#)

- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)³¹⁶⁰.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: Dell OpenManage Server Administrator or iDRAC 7

 This sensor needs the Dell OpenManage Server Administrator tool to be installed on the Dell PowerEdge server to monitor it. Please make sure that you enable SNMP in the OpenManage Server Administrator.

 For details, see the Knowledge Base: [What do I need to monitor Dell servers?](#)

 You can also monitor Dell PowerEdge servers with this sensor type via Integrated Dell Remote Access Controller (iDRAC) 7.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Dell PowerEdge chassis you want to monitor. PRTG will create one sensor for each chassis you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL POWEREDGE SYSTEM HEALTH SPECIFIC

Chassis	Select the chassis you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
---------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DELL POWEREDGE SYSTEM HEALTH SPECIFIC

Chassis	Shows the chassis that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
---------	---

DELL POWEREDGE SYSTEM HEALTH SPECIFIC

Channel Mask	Shows the channel mask that describes which sensors are available. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Data Source	Shows the interface that is used to get monitoring data. This is either Dell OpenManage Server Administrator (OMSA) or Integrated Dell Remote Access Controller (iDRAC).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- ❗ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What do I need to monitor Dell servers?

- <https://kb.paessler.com/en/topic/45333>

Knowledge Base: I can't add Dell PowerEdge sensors to PRTG. What can I do?

- <https://kb.paessler.com/en/topic/68040>

Knowledge Base: Why does my Dell PowerEdge System Health sensor show a power unit status error after iDRAC update?

- <https://kb.paessler.com/en/topic/72855>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
147 SNMP Dell PowerEdge System Health Sensor

Others

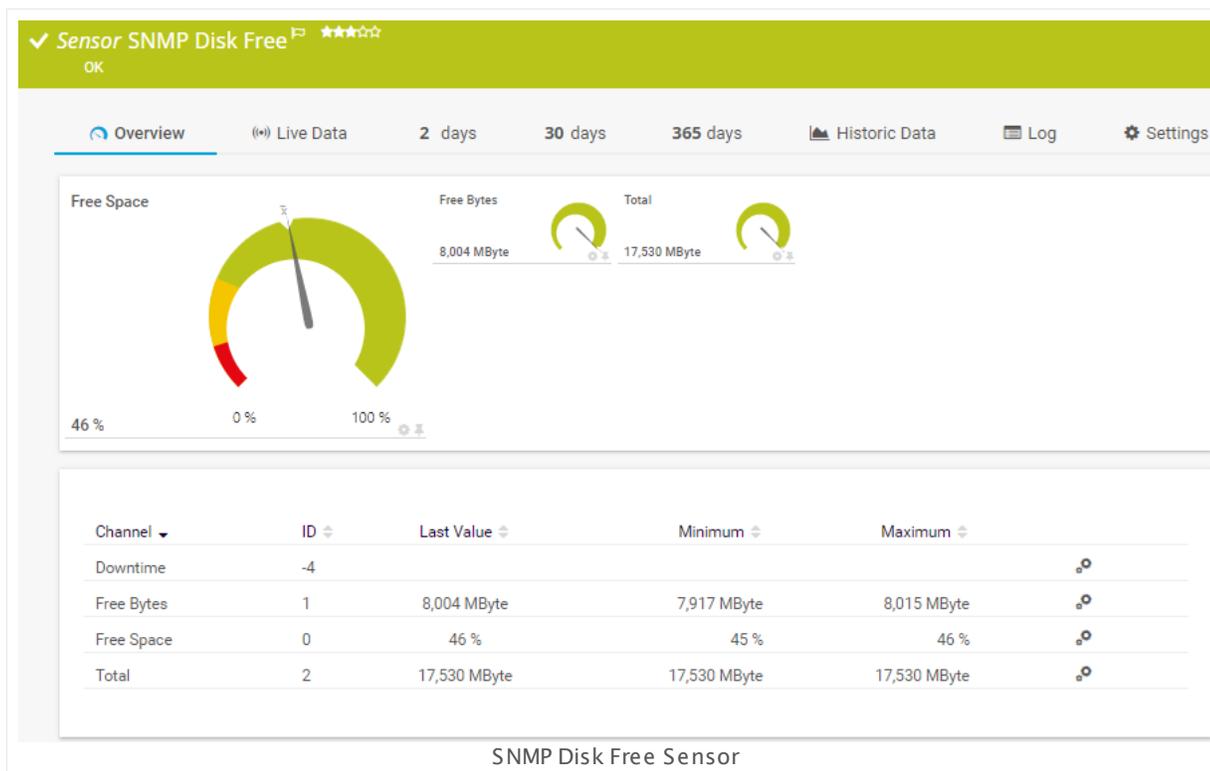
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.148 SNMP Disk Free Sensor

The SNMP Disk Free sensor monitors the free disk space on a logical disk via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in percent
- Free disk space in bytes
- Total disk space



Sensor in Other Languages

Dutch: **SNMP vrije schijf ruimte**, French: **Espace disque disponible SNMP**, German: **SNMP Datenträgerspeicher**, Japanese: **SNMP ? ? ? ? ? ? ? ?**, Portuguese: **Disco livre SNMP**, Russian: **Свободное пространство по SNMP**, Simplified Chinese: **SNMP ? ? ? ? ? ? ? ?**, Spanish: **SNMP Disco libre**

Remarks

- This sensor uses more generic Object Identifier (OID) values compared to the [SNMP Linux Disk Free Sensor](#).
- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DISK FREE SETTINGS

Disk	Select one or more disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
-------------	--

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DISK FREE SETTINGS

Disk	Shows the name of the disk that this sensor is monitoring. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!
------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

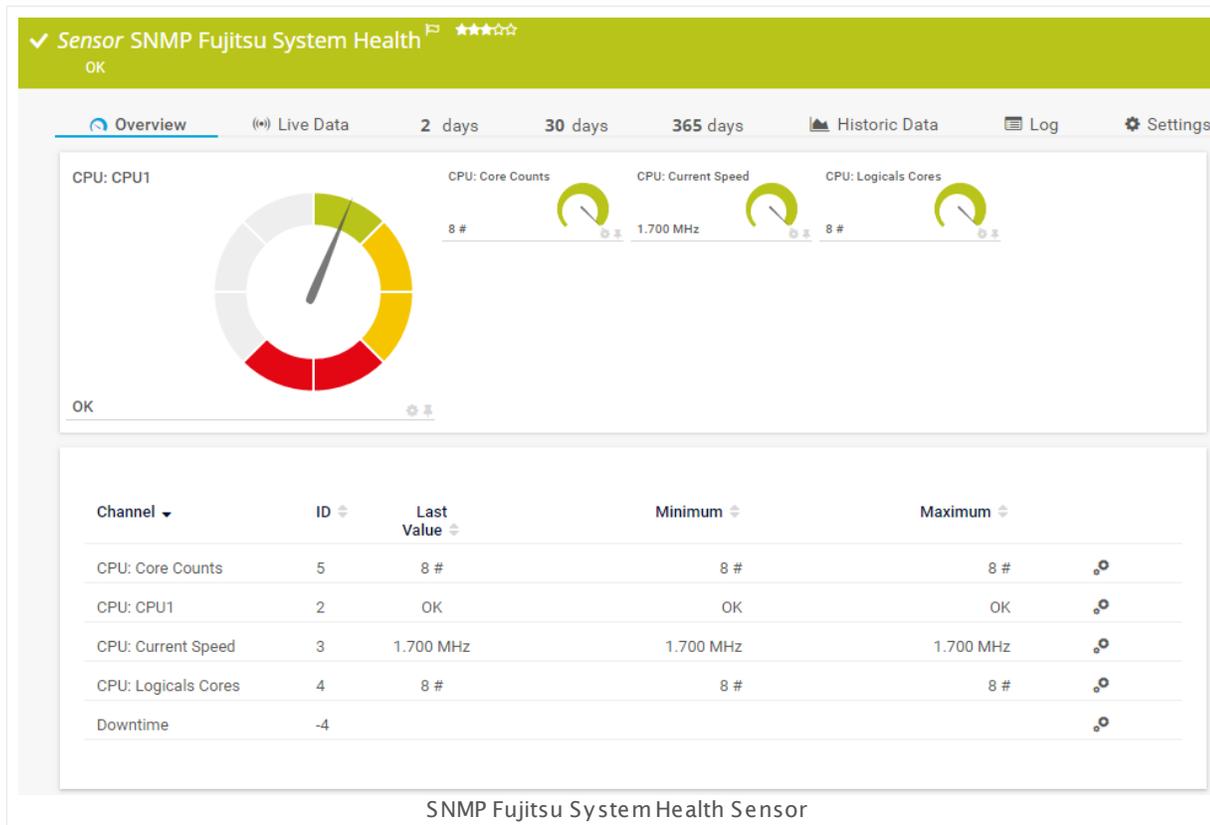
7.8.149 SNMP Fujitsu System Health Sensor

The SNMP Fujitsu System Health sensor monitors the status of a Fujitsu PRIMERGY server via the integrated Remote Management Controller (iRMC) and Simple Network Management Protocol (SNMP). The sensor might also work on other Fujitsu devices that have an iRMC available like PRIMEQUEST servers, some storage systems of the ETERNUS product line, and CELSIUS workstations in racks.

It can show the following:

- Overall status
- CPU status, speed, and core count
- Fan status and speed
- Memory module status
- Number of correctable and uncorrectable errors of the memory module
- Battery status
- Status and condition of the power supply
- Power limit status and power consumption
- Temperatures for various components of the server, for example, memory, power supply, CPU, system, and storage.

These channels are created at run-time, depending on the available measurement components. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Remarks

- Use an iRMC interface as parent device for this sensor.
- Please make sure to enable SNMP in the iRMC via ServerView.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- **BETA** Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the measurements you want to monitor. PRTG will create one sensor for each measurement you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

FUJITSU SYSTEM SPECIFIC

Measurement Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3270], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

FUJITSU SYSTEM SPECIFIC

Measurement Shows the type of measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Identifier Shows the value that identifies the row in the table. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

i The identifier has the following format: **RowIndex | Unique | Measurement**. For example, **1.1|BATT 3.0V|Voltage**.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

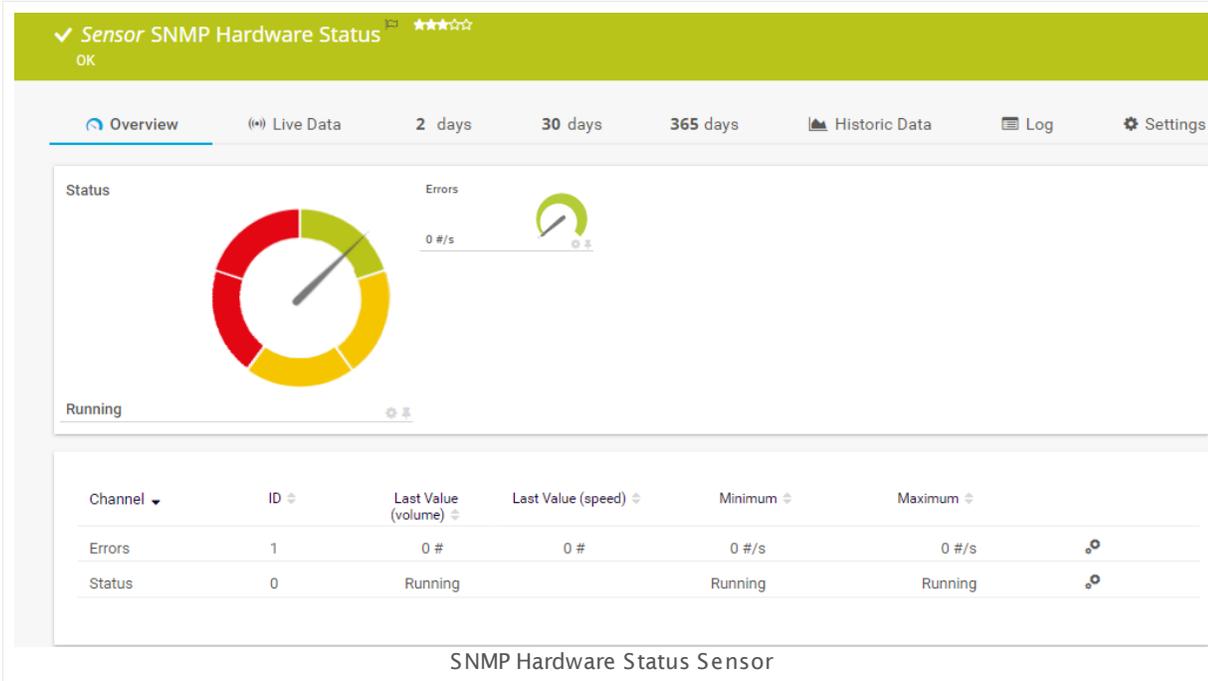
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.150 SNMP Hardware Status Sensor

The SNMP Hardware Status sensor monitors the status of a hardware component of a server via Simple Network Management Protocol (SNMP).

It shows the following:

- Current status of the monitored hardware component
- Number of errors per time period



Sensor in Other Languages

Dutch: **SNMP Hardware Status**, French: **Statut matériel SNMP**, German: **SNMP Hardwarezustand**, Japanese: **SNMP ? ? ? ? ? ? ? ?**, Portuguese: **Status do hardware SNMP**, Russian: **Статус оборудования по SNMP**, Simplified Chinese: **SNMP ? ? ? ?**, Spanish: **Estado del hardware de SNMP**

Remarks

- It might not work to query data from a probe device via SNMP (querying **localhost**, **127.0.0.1**, or **:::1**). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the hardware components you want to monitor. PRTG will create one sensor for each component you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HARDWARE SPECIFIC

Hardware Component	Select the hardware components you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

HARDWARE SPECIFIC

Hardware Component	Shows further information about the hardware component. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Product ID	
Description	
Type	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
150 SNMP Hardware Status Sensor

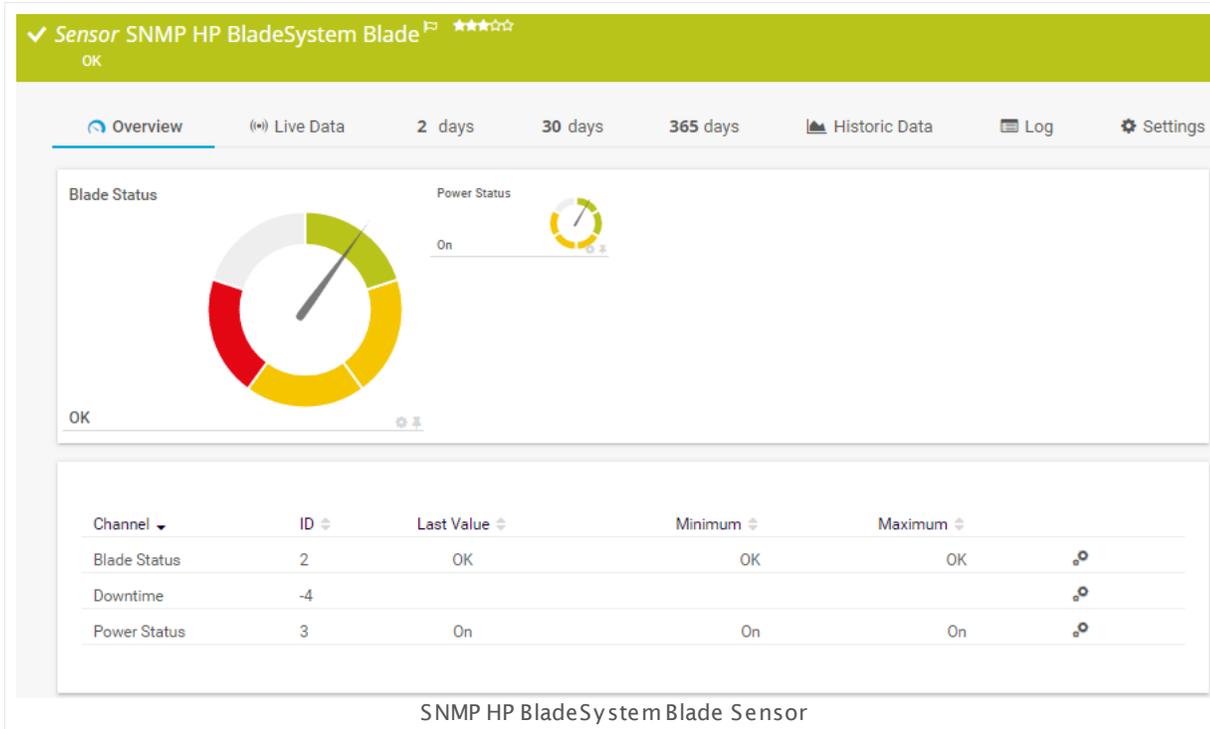
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.151 SNMP HP BladeSystem Blade Sensor

The SNMP HP BladeSystem Blade sensor monitors the status of an HP BladeSystem via Simple Network Management Protocol (SNMP). It can show the following:

- Blade status (OK, degraded, unknown, failed, other)
- Power status (OK, on, off, power staged off, unknown, other)



Sensor in Other Languages

Dutch: **SNMP HP BladeSystem Blade**, French: **Lame HP BladeSystem SNMP**, German: **SNMP HP BladeSystem Blade**, Japanese: **SNMP HP ? ? ? ? ? ? ? ? ? ? ? ?**, Portuguese: **Blade do SNMP HP BladeSystem**, Russian: **Блейд-модуль HP BladeSystem по SNMP**, Simplified Chinese: **SNMP HP BladeSystem ? ?**, Spanish: **Blade de SNMP de HP BladeSystem**

Remarks

- Make sure you add this sensor to a device whose IP/DNS name points to the HP BladeSystem Enclosure hosting the Onboard Administrator!
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the server blades you want to monitor. PRTG will create one sensor for each blade you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP BLADESYSTEM SPECIFIC

Server Blade	Select the blades you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[213] , logs ^[228] , notifications ^[3216] , reports ^[3262] , maps ^[3270] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP BLADESYSTEM SPECIFIC

- Server Blade** Shows the server blade that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

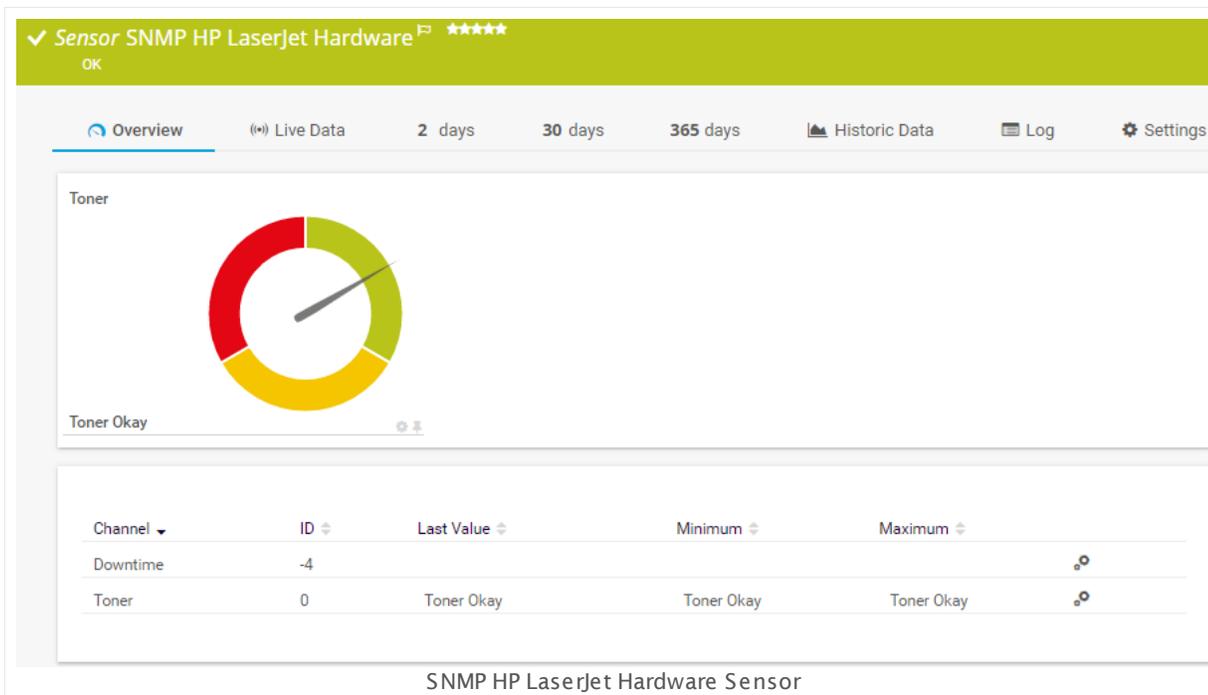
7.8.153 SNMP HP LaserJet Hardware Sensor

The SNMP HP LaserJet Hardware sensor monitors performance counters on a HP LaserJet hardware device using Simple Network Management Protocol (SNMP).

It can show the following, depending on what category you monitor:

- Status of toner
- Status of paper
- Paper jam status

 The SNMP HP LaserJet Hardware sensor will not appear as running sensor, instead it will be created as [SNMP Custom Advanced sensor](#)¹⁹⁵⁹.



Sensor in Other Languages

Dutch: **SNMP HP LaserJet Hardware**, French: **Matériels SNMP HP LaserJet**, German: **SNMP HP LaserJet Hardware**, Japanese: **SNMP HP LaserJet** ? ? ? ? ? ? , Portuguese: **Hardware da HP LaserJet SNMP**, Russian: **Оборудование HP LaserJet по SNMP**, Simplified Chinese: **SNMP HP LaserJet** ? ? , Spanish: **Hardware SNMP HP LaserJet**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the categories you want to monitor. PRTG will create one [SNMP Custom Advanced sensor](#) including all performance counters you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DELL HARDWARE SPECIFIC

Library OIDs

Select the categories you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The following performance counters for your printer are available:

- **Toner/Status**
- **Paper/Status**
- **Jam/Status**

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP LASERJET SPECIFIC

Selected Interface	Shows the name of the category (performance counter) that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification whenever the sensor value changes.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
153 SNMP HP LaserJet Hardware Sensor

Others

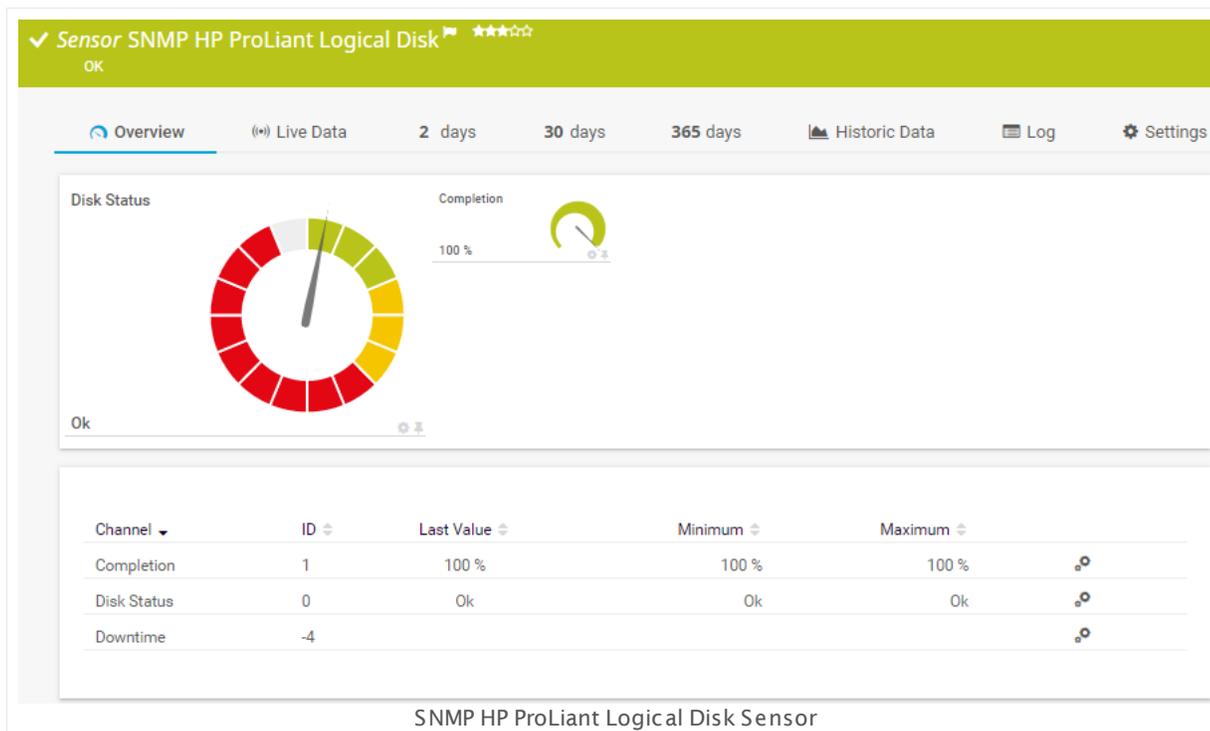
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.154 SNMP HP ProLiant Logical Disk Sensor

The SNMP HP ProLiant Logical Disk sensor monitors a logical disk in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Disk status
- Completion in percent: This is only important when the disk status is "Reconstructing" or "Expanding" and illustrates the progress of this task.



Sensor in Other Languages

Dutch: **SNMP HP ProLiant logische schijf**, French: **Disque logique HP ProLiant SNMP**, German: **SNMP HP ProLiant Logischer Datenträger**, Japanese: **SNMP HP ProLiant ? ? ? ?**, Portuguese: **Disco lógico SNMP HP ProLiant**, Russian: **Логический диск HP ProLiant по SNMP**, Simplified Chinese: **SNMP HP ProLiant ? ? ? ?**, Spanish: **Disco lógico SNMP HP ProLiant**

Remarks

- For Gen9 servers or earlier: [Requires](#) ²¹¹⁸ HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- For Gen10 servers: [Requires](#) ²¹¹⁸ HPE Agentless Management and the HPE Agentless Management Service to be installed on the target device.
- For Gen10 servers: [Use the HP iLO interface](#) ²¹¹⁸ as parent device for this sensor.

- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** or later.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: HP System Management Tools

For Gen9 servers or earlier, this sensor needs a specific HP system management tool to be installed on the target device to report data via SNMP: **HP Insight Management Agents**. To receive SNMP data from RAID controllers, you additionally need **HP Insight Management WBEM Providers**. For Gen10 servers, this sensor no longer requires HP system management tools. Instead, the sensor needs the Agentless Management Service to be installed on the target device.

 For more details and download links, see the Knowledge Base: [Monitor HP ProLiant via SNMP?](#)

 For Gen9 servers or earlier, some of the HP **Object Identifiers (OIDs)** that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**. For Gen10 servers, use the HP iLO interface as parent device for this sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks in the HP server you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT LOGICAL DISK SETTINGS

Disk Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT LOGICAL DISK SETTINGS

Disk Shows the name of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <https://kb.paessler.com/en/topic/33133>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.155 SNMP HP ProLiant Memory Controller Sensor

The SNMP HP ProLiant Memory Controller sensor monitors a memory controller in an HP server via Simple Network Management Protocol (SNMP).

It shows the following:

- Error status of the controller
- Condition of the controller
- States and conditions of available modules.

✓ Sensor SNMP HP ProLiant Memory Controller ★★★★☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Controller Error Status



Advanced Ecc

Controller Condition



OK

Module 2 Condition



OK

Module 2 Status



Good

Module 3 Condition



OK

Module 3 Status



Good

Module 5 Condition



OK

Module 5 Status



Good

Module 6 Condition



OK

Module 6 Status



Good

Module 8 Condition



OK

Module 8 Status



Good

Module 9 Condition



OK

Module 9 Status



Good

Channel	ID	Last Value	Minimum	Maximum	
Controller Condition	1	OK	OK	OK	
Controller Error Status	0	Advanced Ecc	Advanced Ecc	Advanced Ecc	
Downtime	-4				
Module 2 Condition	3	OK	OK	OK	
Module 2 Status	2	Good	Good	Good	
Module 3 Condition	5	OK	OK	OK	
Module 3 Status	4	Good	Good	Good	
Module 5 Condition	7	OK	OK	OK	
Module 5 Status	6	Good	Good	Good	
Module 6 Condition	9	OK	OK	OK	

SNMP HP ProLiant Memory Controller Sensor

Sensor in Other Languages

Dutch: **SNMP HP ProLiant Memory Controller**, French: **Contrôleur de mémoire HP Proliant SNMP**, German: **SNMP HP ProLiant Speichercontroller**, Japanese: **SNMP HP Proliant ? ? ? ? ? ? ?**, Portuguese: **Controlador de memória SNMP HP Proliant**, Russian: **Контроллер памяти HP Proliant по SNMP**, Simplified Chinese: **SNMP HP Proliant ? ? ? ? ?**, Spanish: **Controlador de memoria SNMP HP Proliant**

Remarks

- For Gen9 servers or earlier: [Requires](#)²¹²⁷ HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- For Gen10 servers: [Requires](#)²¹²⁷ HPE Agentless Management and the HPE Agentless Management Service to be installed on the target device.
- For Gen10 servers: [Use the HP iLO interface](#)²¹²⁷ as parent device for this sensor.
- Knowledge Base: [Which lookup values are supported by the SNMP HP ProLiant Memory Controller Sensor?](#)
- If modules are inserted at a later point, you have to add this sensor anew.
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** or later.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: HP System Management Tools

For Gen9 servers or earlier, this sensor needs a specific HP system management tool to be installed on the target device to report data via SNMP: **HP Insight Management Agents**. To receive SNMP data from RAID controllers, you additionally need **HP Insight Management WBEM Providers**. For Gen10 servers, this sensor no longer requires HP system management tools. Instead, the sensor needs the Agentless Management Service to be installed on the target device.

 For more details and download links, see the Knowledge Base: [Monitor HP ProLiant via SNMP?](#)

 For Gen9 servers or earlier, some of the HP **Object Identifiers (OIDs)** that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**. For Gen10 servers, use the HP iLO interface as parent device for this sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory controllers in the HP server you want to monitor. PRTG will create one sensor for each controller you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT MEMORY CONTROLLER SETTINGS

Controller Select the controllers you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT MEMORY CONTROLLER SETTINGS

Controller Shows the name of the controller that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <https://kb.paessler.com/en/topic/33133>

Knowledge Base: Which lookup values are supported by the SNMP HP ProLiant Memory Controller Sensor?

- <https://kb.paessler.com/en/topic/44803>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

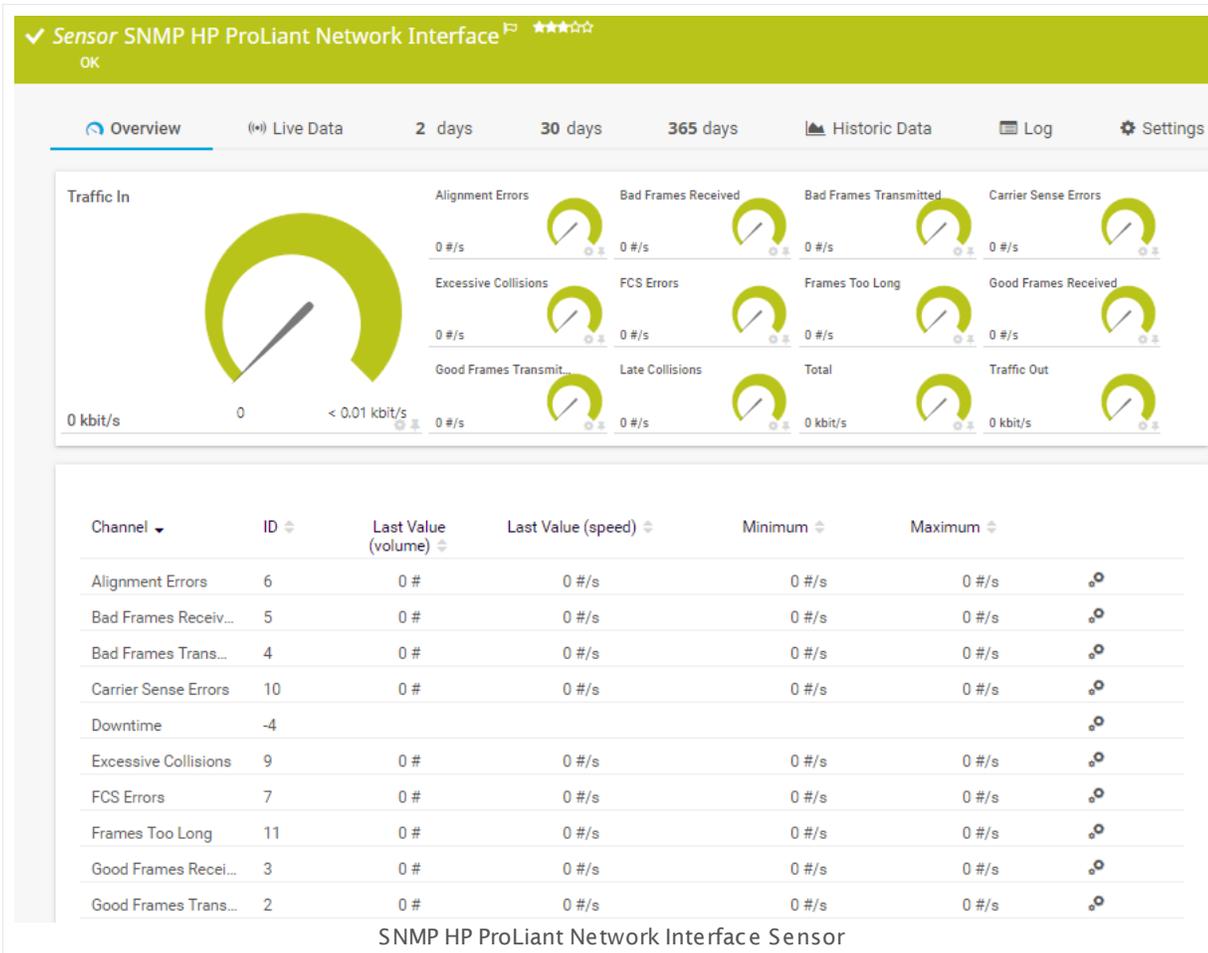
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.156 SNMP HP ProLiant Network Interface Sensor

The SNMP HP ProLiant Network Interface sensor monitors a network interface in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Traffic in
- Traffic out
- Number of transmitted and received good frames
- Number of transmitted and received bad frames
- Alignment errors
- FCS (Frame Check Sequence) errors
- Late and excessive collisions
- Carrier sense errors
- If frames are too long



Sensor in Other Languages

Dutch: **SNMP HP ProLiant Network Interface**, French: **Interface réseau HP ProLiant SNMP**, German: **SNMP HP ProLiant Netzwerkschnittstelle**, Japanese: **SNMP HP ProLiant ? ? ? ? ? ? ? ? ? ? ? ? ? ?**, Portuguese: **Interface de rede SNMP HP ProLiant**, Russian: **Сетевой интерфейс HP ProLiant по SNMP**, Simplified Chinese: **SNMP HP ProLiant ? ? ? ?**, Spanish: **SNMP Interface de red HP ProLiant**

Remarks

- For Gen9 servers or earlier: [Requires](#)²¹³⁷ HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- For Gen10 servers: [Requires](#)²¹³⁷ HPE Agentless Management and the HPE Agentless Management Service to be installed on the target device.
- For Gen10 servers: [Use the HP iLO interface](#)²¹³⁷ as parent device for this sensor.
- When adding the sensor, the status of each available network interface is shown. If this status is **Link Failure**, it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface will not work correctly. The error message in this case will be "No Such Name (SNMP error # 2)".
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** or later.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: HP System Management Tools

For Gen9 servers or earlier, this sensor needs a specific HP system management tool to be installed on the target device to report data via SNMP: **HP Insight Management Agents**. To receive SNMP data from RAID controllers, you additionally need **HP Insight Management WBEM Providers**. For Gen10 servers, this sensor no longer requires HP system management tools. Instead, the sensor needs the Agentless Management Service to be installed on the target device.

 For more details and download links, see the Knowledge Base: [Monitor HP ProLiant via SNMP?](#)

 For Gen9 servers or earlier, some of the HP **Object Identifiers (OIDs)** that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**. For Gen10 servers, use the HP iLO interface as parent device for this sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network interfaces in the HP server you want to monitor. PRTG will create one sensor for each interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT NETWORK INTERFACE SETTINGS

Network Interface Select the interfaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

i If this status is **Link Failure**, it is still possible to add a sensor for the respective interface. Though, most likely the sensor for this interface will not work correctly. The error message in this case will be **No Such Name (SNMP error # 2)**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT NETWORK INTERFACE SETTINGS

Network Interface	Shows the name of the interface that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.</p>
Chart Type	Define how to show different channels for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ❗ You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.
- **Show in and out traffic as positive and negative area chart:** Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way.
 - ❗ You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.
 - ❗ You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the [Sensor Channels Settings](#)³¹⁶⁰).

Stack Unit

This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) ³³⁸⁵ on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status** ¹⁹⁵¹. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) ³⁶⁸³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <https://kb.paessler.com/en/topic/33133>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

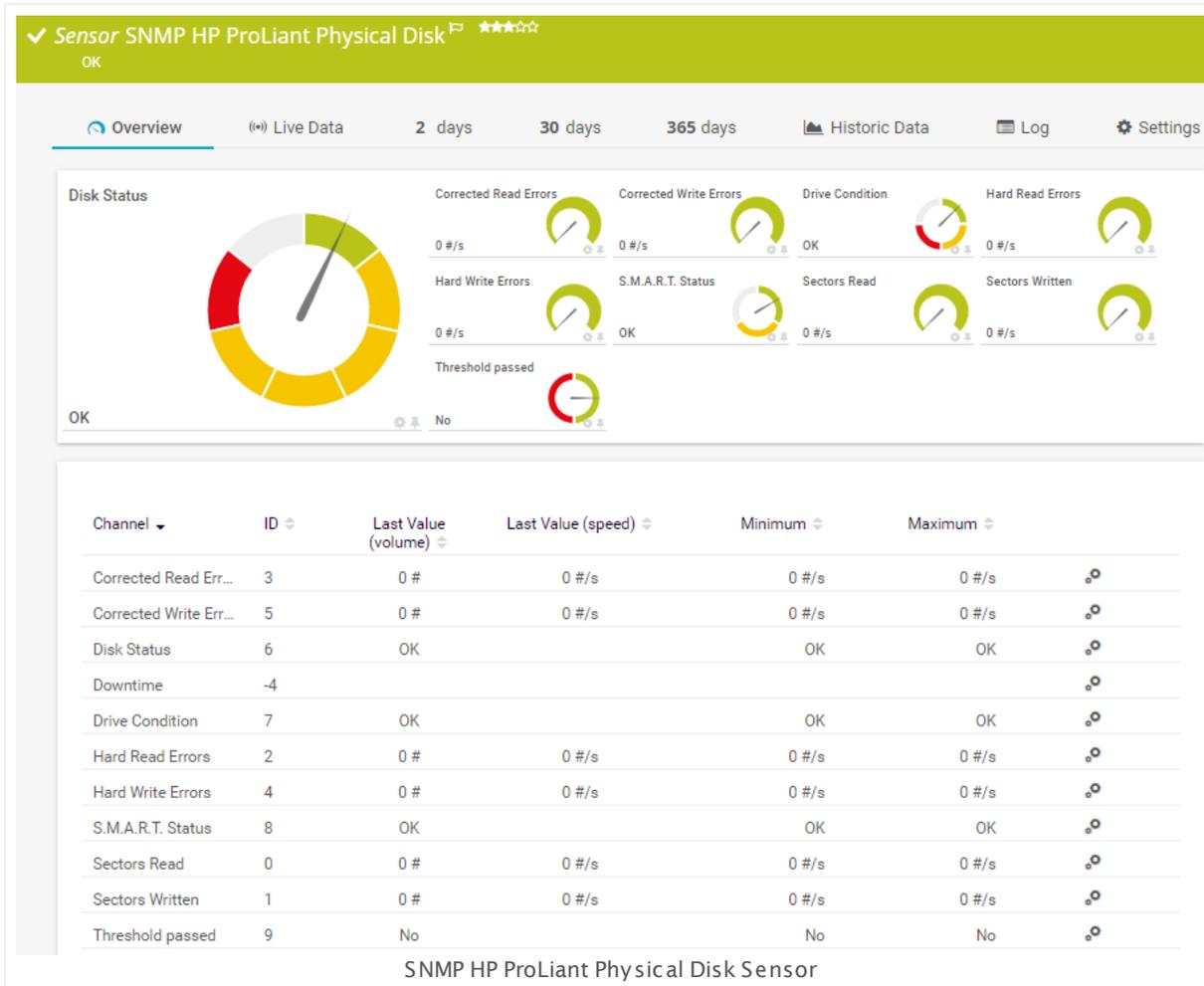
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.157 SNMP HP ProLiant Physical Disk Sensor

The SNMP HP ProLiant Physical Disk sensor monitors a physical disk in an HP server via Simple Network Management Protocol (SNMP).

It can show the following:

- Read and written sectors
- Hard and corrected read errors
- Hard and corrected write errors
- Disk status
 - **Up:** ok
 - **Warning:** predictive failure, erasing, erase done, erase queued, not authenticated
 - **Down:** failed, SSD wear out
- Drive condition
- Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status
- If the threshold is passed



Sensor in Other Languages

Dutch: **SNMP HP ProLiant Fysieke Schijf**, French: **Disque physique HP Proliant SNMP**, German: **SNMP HP Proliant Physikalischer Datenträger**, Japanese: **SNMP HP Proliant ? ? ? ? ?**, Portuguese: **Disco fisico SNMP HP ProLiant**, Russian: **Физический диск HP ProLiant no SNMP**, Simplified Chinese: **SNMP HP Proliant ? ? ? ?**, Spanish: **SNMP Disco fisico HP Proliant**

Remarks

- For Gen9 servers or earlier: [Requires](#) ²¹⁴⁸ HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- For Gen10 servers: [Requires](#) ²¹⁴⁸ HPE Agentless Management and the HPE Agentless Management Service to be installed on the target device.
- For Gen10 servers: [Use the HP iLO interface](#) ²¹⁴⁸ as parent device for this sensor.
- The sensor will only show **Disk Status** and no other channels if it runs in "Limited Monitoring" mode. For more information, see [SNMP HP ProLiant Physical Disk sensor not showing all information](#).

- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** or later.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: HP System Management Tools

For Gen9 servers or earlier, this sensor needs a specific HP system management tool to be installed on the target device to report data via SNMP: **HP Insight Management Agents**. To receive SNMP data from RAID controllers, you additionally need **HP Insight Management WBEM Providers**. For Gen10 servers, this sensor no longer requires HP system management tools. Instead, the sensor needs the Agentless Management Service to be installed on the target device.

 For more details and download links, see the Knowledge Base: [Monitor HP ProLiant via SNMP?](#)

 For Gen9 servers or earlier, some of the HP **Object Identifiers (OIDs)** that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**. For Gen10 servers, use the HP iLO interface as parent device for this sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the HP server you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

HP PROLIANT PHYSICAL DISK SETTINGS

Disk Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

HP PROLIANT PHYSICAL DISK SETTINGS

Disk Shows the identifier of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
-  Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
-  If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
-  If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <https://kb.paessler.com/en/topic/33133>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: SNMP HP ProLiant Physical Disk sensor not showing all information

- <https://kb.paessler.com/en/topic/70009>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.158 SNMP HP ProLiant System Health Sensor

The SNMP HP ProLiant System Health sensor monitors the system health of an HP ProLiant server via Simple Network Management Protocol (SNMP).

It can show the following:

- Overall status
- Thermal status
- System fan status
- CPU fan status
- Number of broken and running fans
- Number of broken and running fans that are fault tolerant
- Status and condition of the power supply
- Temperatures for various components of the server, for example, memory, power supply, CPU, system, and storage.
- Power consumption
- Disk controller status

These channels are created at run-time, depending on the available measurement components. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ **Sensor SNMP HP ProLiant System Health** ★★★★☆

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Overall Status



OK

CPU Fan Status		Other	OK
Disk Controller Status		OK	OK
Fans Broken		0 #	0 #
Fans Running		0 #	0 #
Fault Tolerant Fans Bro		0 #	0 #
Fault Tolerant Fans Ru		3 #	3 #
Integrated Manageme...		Undefined lookup v...	Undefined lookup v...
Power Consumption 1		22 %	22 %
Power Supply 1 Condi...		OK	OK
Power Supply 1 Status		No Error	No Error
System Fan Status		OK	OK
Temperature 01(ambie)		21 °C	21 °C
Temperature 02(cpu)		40 °C	40 °C
Temperature 04(memo)		35 °C	35 °C
Temperature 05(memo)		36 °C	36 °C
Temperature 06(memo)		36 °C	36 °C
Temperature 07(memo)		34 °C	34 °C
Temperature 09(memo)		32 °C	32 °C
Temperature 11(memo)		32 °C	32 °C
Temperature 12(power)		34 °C	34 °C
Temperature 13(power)		48 °C	48 °C
Temperature 14(memo)		29 °C	29 °C
Temperature 15(cpu)		32 °C	32 °C
Temperature 16(cpu)		32 °C	32 °C
Temperature 17(memo)		28 °C	28 °C
Temperature 18(cpu)		40 °C	40 °C
Temperature 19(system)		39 °C	39 °C
Temperature 20(system)		39 °C	39 °C
Temperature 21(system)		46 °C	46 °C
Temperature 22(system)		47 °C	47 °C
Temperature 23(system)		42 °C	42 °C
Temperature 24(system)		50 °C	50 °C
Temperature 25(system)		36 °C	36 °C
Temperature 26(system)		49 °C	49 °C
Temperature 27(storag)		35 °C	35 °C
Temperature 28(system)		73 °C	73 °C
Thermal Status		OK	OK

Channel	ID	Last Value	Minimum	Maximum	
CPU Fan Status	3	Other	Other	Other	
Disk Controller Status	1030	OK	OK	OK	
Downtime	-4				
Fans Broken	5	0 #	0 #	0 #	
Fans Running	4	0 #	0 #	0 #	

SNMP HP ProLiant System Health Sensor

Sensor in Other Languages

Dutch: **SNMP HP ProLiant Systeemstatus**, French: **État du système HP ProLiant SNMP**, German: **SNMP HP Proliant Systemzustand**, Japanese: **SNMP HP Proliant ? ? ? ? ? ? ?** , Portuguese: **Funcionamento do sistema SNMP HP ProLiant** , Russian: **Работоспособность системы HP ProLiant по SNMP**, Simplified Chinese: **SNMP HP Proliant ? ? ? ? ? ? ?** , Spanish: **SNMP Salud de sistema HP Proliant**

Remarks

- For Gen9 servers or earlier: [Requires](#) ²¹⁵⁸ HP Insight Management Agents and HP Insight Management WBEM Providers to be installed on the target device.
- For Gen10 servers: [Use the HP iLO interface](#) ²¹⁵⁸ as parent device for this sensor.

8/14/2018

2157

- This sensor has predefined limits for temperatures and broken frames. You can change these limits individually in the [channel settings](#)^[3160].
- RAID controllers that have no hard disks assigned might cause a **Down status**^[195]. In this case, deactivate the respective controller(s) in the HP ProLiant BIOS to avoid sensor errors.
- This sensor type supports monitoring HP Integrated Lights-Out (iLO) as of iLO version 3. We recommend that you use **iLO 4** or later.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Requirement: HP System Management Tools

For Gen9 servers or earlier, this sensor needs a specific HP system management tool to be installed on the target device to report data via SNMP: **HP Insight Management Agents**. To receive SNMP data from RAID controllers, you additionally need **HP Insight Management WBEM Providers**. For Gen10 servers, this sensor no longer requires HP system management tools.

 For more details and download links, see the Knowledge Base: [Monitor HP ProLiant via SNMP?](#)

 For Gen9 servers or earlier, some of the HP **Object Identifiers (OIDs)** that this sensor type uses are only accessible via the HP Integrated Lights-Out (iLO) interface. If this sensor throws an error that it cannot find "such device types", please create a device in PRTG that points to the address of the HP iLO interface (if available) and add the sensor to this device. We recommend that you use the **Agentless Management** feature with configured SNMP. You can set this up in the iLO configuration interface under **Administration | Management | SNMP Settings**. For Gen10 servers, use the HP iLO interface as parent device for this sensor.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Monitor HP ProLiant via SNMP

- <https://kb.paessler.com/en/topic/33133>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why is my SNMP HP ProLiant System Health sensor in error status after updating PRTG?

- <https://kb.paessler.com/en/topic/61805>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.159 SNMP IBM System X Logical Disk Sensor

The SNMP IBM System X Logical Disk sensor monitors a logical disk in an IBM server via Simple Network Management Protocol (SNMP).

- It shows the status of a logical disk in an IBM server.

✓ Sensor SNMP IBM System X Logical Disk ★★★★☆
OK

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Disk Status

Ok

Channel	ID	Last Value	Minimum	Maximum
Disk Status	0	Ok	Ok	Ok
Downtime	-4			

SNMP IBM System X Logical Disk Sensor

Sensor in Other Languages

Dutch: **SNMP IBM System X Logical Disk**, French: **Disque logique IBM System X SNMP**, German: **SNMP IBM System X Logischer Datenträger**, Japanese: **SNMP IBM System X ? ? ? ? ?**, Portuguese: **Disco lógico do IBM System X SNMP**, Russian: **Логический диск IBM System X no SNMP**, Simplified Chinese: **SNMP IBM ? ? X ? ? ? ?**, Spanish: **Disco lógico de IBM System X con SNMP**

Remarks

- [Requires](#)²¹⁶⁷ the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: [What are the requirements to monitor IBM System x?](#)
- Knowledge Base: [IBM System X sensors could not find any disk/data on this device \(PE187/PE188/PE194\)](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Requirement: IBM Systems Director Platform Agent

-  This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device to monitor it via SNMP.
-  For more information, see the Knowledge Base: [What are the requirements to monitor IBM System x?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks of the IBM device you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X LOGICAL DISK SETTINGS

Disk	Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

-  Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X LOGICAL DISK SETTINGS

Disk	Shows the ID of the logical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------	--

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

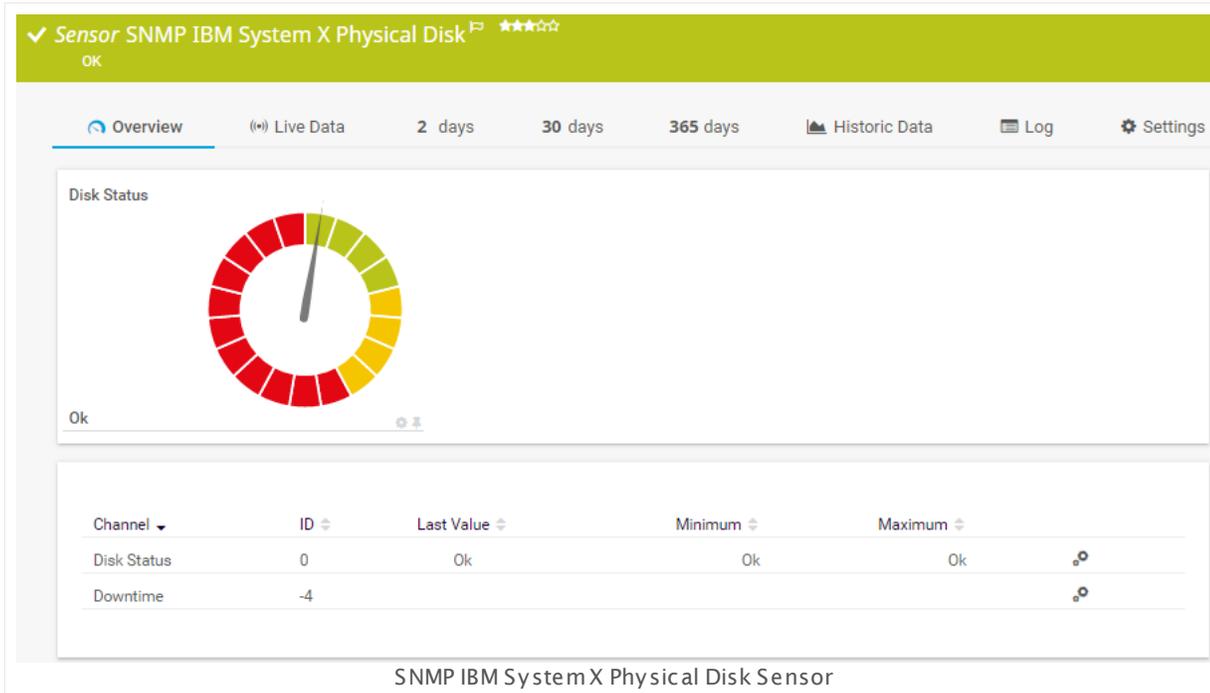
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.160 SNMP IBM System X Physical Disk Sensor

The SNMP IBM System X Physical Disk sensor monitors a physical disk in an IBM server via Simple Network Management Protocol (SNMP).

- It shows the status of a physical disk.



Sensor in Other Languages

Dutch: **SNMP IBM System X Physical Disk**, French: **Disques physiques IBM System X SNMP**, German: **SNMP IBM System X Physikalischer Datenträger**, Japanese: **SNMP IBM System X** ? ? ? ? ? ? , Portuguese: **Disco físico do IBM System X SNMP**, Russian: **Физический диск IBM System X no SNMP**, Simplified Chinese: **SNMP IBM ? ? X ? ? ? ?** , Spanish: **Disco físico de IBM System X con SNMP**

Remarks

- [Requires](#)^[2176] the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: [What are the requirements to monitor IBM System x?](#)
- Knowledge Base: [IBM System X sensors could not find any disk/data on this device \(PE187/PE188/PE194\)](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Requirement: IBM Systems Director Platform Agent

-  This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device to monitor it via SNMP.
-  For more information, see the Knowledge Base: [What are the requirements to monitor IBM System x?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks of the IBM device you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X PHYSICAL DISK SETTINGS

Disk	Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

-  Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X PHYSICAL DISK SETTINGS

Disk	Shows the ID of the physical disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------	---

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

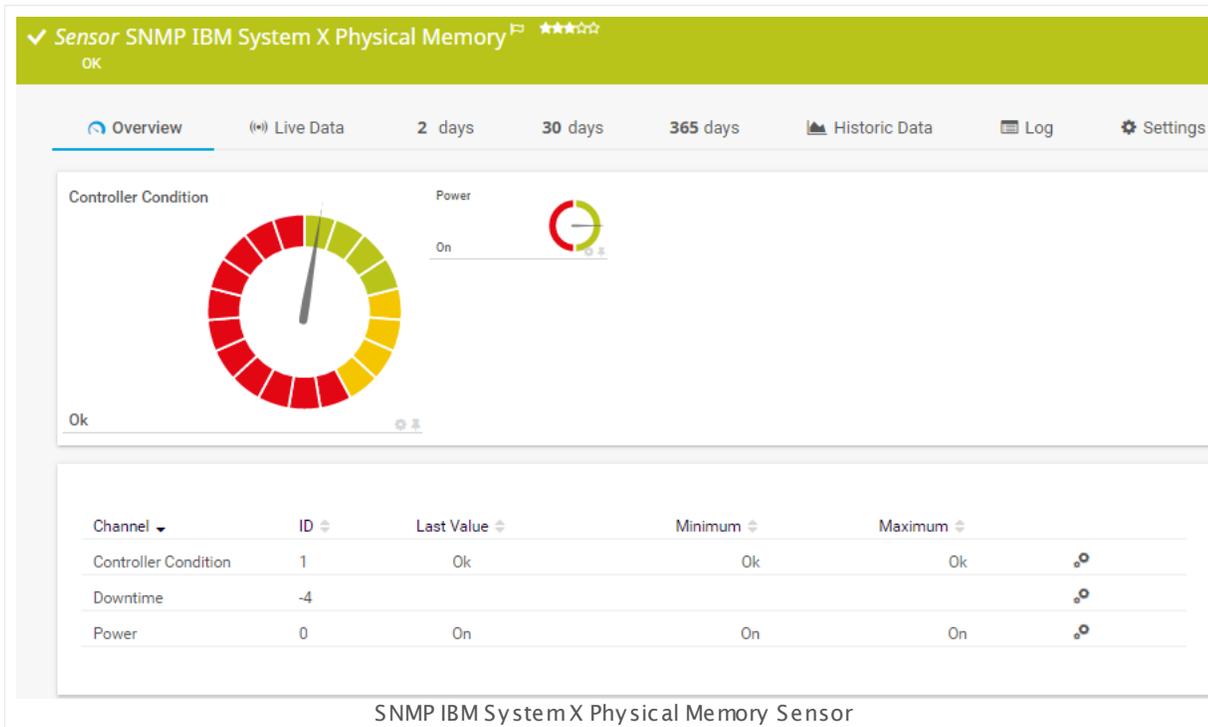
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.161 SNMP IBM System X Physical Memory Sensor

The SNMP IBM System X Physical Memory sensor monitors the memory modules in an IBM server via Simple Network Management Protocol (SNMP).

It shows the following:

- Condition of memory controller
- Power status (on or off)



Sensor in Other Languages

Dutch: **SNMP IBM System X Physical Memory**, French: **Mémoire physique SNMP IBM System X**, German: **SNMP IBM System X Physikalischer Speicher**, Japanese: **SNMP IBM System X ? ? ? ? ?**, Portuguese: **Memória física do IBM System X SNMP**, Russian: **Физическая память IBM System X по SNMP**, Simplified Chinese: **SNMP IBM ? ? X ? ? ? ?**, Spanish: **Memoria física de IBM System X con SNMP**

Remarks

- [Requires](#) ²¹⁸⁵ the IBM Systems Director Platform to be installed on the target device.
- Knowledge Base: [What are the requirements to monitor IBM System x?](#)
- Knowledge Base: [IBM System X sensors could not find any disk/data on this device \(PE187/PE188/PE194\)](#)

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Requirement: IBM Systems Director Platform Agent

- ✘ This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device to monitor it via SNMP.
- 💡 For more information, see the Knowledge Base: [What are the requirements to monitor IBM System x?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory modules of the IBM server you want to monitor. PRTG will create one sensor for each module you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X PHYSICAL MEMORY SETTINGS

Module	Select the memory modules you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ❗ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X PHYSICAL MEMORY SETTINGS

Name	Shows further information about the module. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Caption	
Serial Number	
Size	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

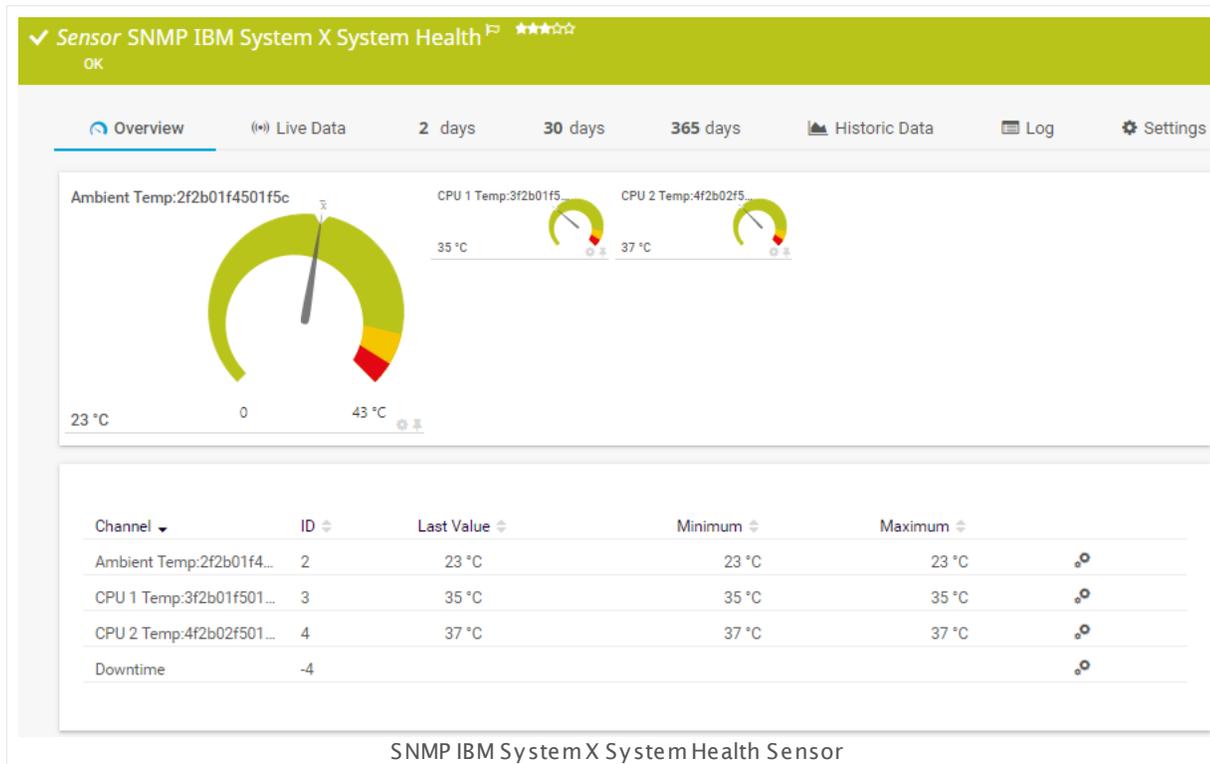
7.8.162 SNMP IBM System X System Health Sensor

The SNMP IBM System X System Health sensor monitors the system health of an IBM device via Simple Network Management Protocol (SNMP).

It can show the following, depending on what measurement you select:

- Overall health
 - **System level or Normal** ([sensor status](#) ¹⁹⁵ Up)
 - **Non Critical** (sensor status **Warning**)
 - **Critical** (sensor status **Down**)
- Temperatures of ambient and CPUs
- Voltages of planars
- Status of power supplies (**OK** or **Error**)
- Fans: RPM (revolutions per minute) or the current percentage of the possible maximum

These channels are created at run-time, depending on the available measurement components. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP IBM System X System Health**, French: **État du système IBM System X SNMP**,

German: **SNMP IBM System X Systemzustand**, Japanese: **SNMP IBM System X ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema IBM System X SNMP**, Russian: **Работоспособность системы IBM System X по SNMP**, Simplified Chinese: **SNMP IBM ? ? X ? ? ? ? ? ?**, Spanish: **Salud del sistema de IBM System X con SNMP**

Remarks

- [Requires](#)^[2194] the IBM Systems Director Platform to be installed on the target device.
- This sensor can also run directly on an **Integrated Management Module (IMM)** network port and can show the overall health on IMMs.
- If the IBM device returns a string in an unexpected format for the percentage of fan revolutions (for example, "offline"), this sensor will show -1% in the corresponding channel. You can define a **Down status**^[195] for this via [channel limits](#)^[3162].
- Knowledge Base: [What are the requirements to monitor IBM System x?](#)
- Knowledge Base: [IBM System X sensors could not find any disk/data on this device \(PE187/PE188/PE194\)](#)
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)^[3160].
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Requirement: IBM Systems Director Platform Agent

- ✘ This sensor type needs the IBM Systems Director Platform Agent to be installed on the target IBM device to monitor it via SNMP.
- 📖 For more information, see the Knowledge Base: [What are the requirements to monitor IBM System x?](#)
- ℹ The SNMP IBM System X System Health sensor can also run directly on an **Integrated Management Module (IMM)** network port and can show the overall health on IMMs.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the measurements of the IBM device you want to monitor. PRTG will create one sensor for each measurement you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

IBM SYSTEM X SYSTEM HEALTH SPECIFIC

Measurement Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

IBM SYSTEM X SYSTEM HEALTH SPECIFIC

Source Shows the source of the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Measurement Shows the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[335] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What are the requirements to monitor IBM System x?

- <https://kb.paessler.com/en/topic/59393>

Knowledge Base: IBM System X sensors could not find any disk/data on this device (PE187/PE188/PE194)

- <https://kb.paessler.com/en/topic/73914>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

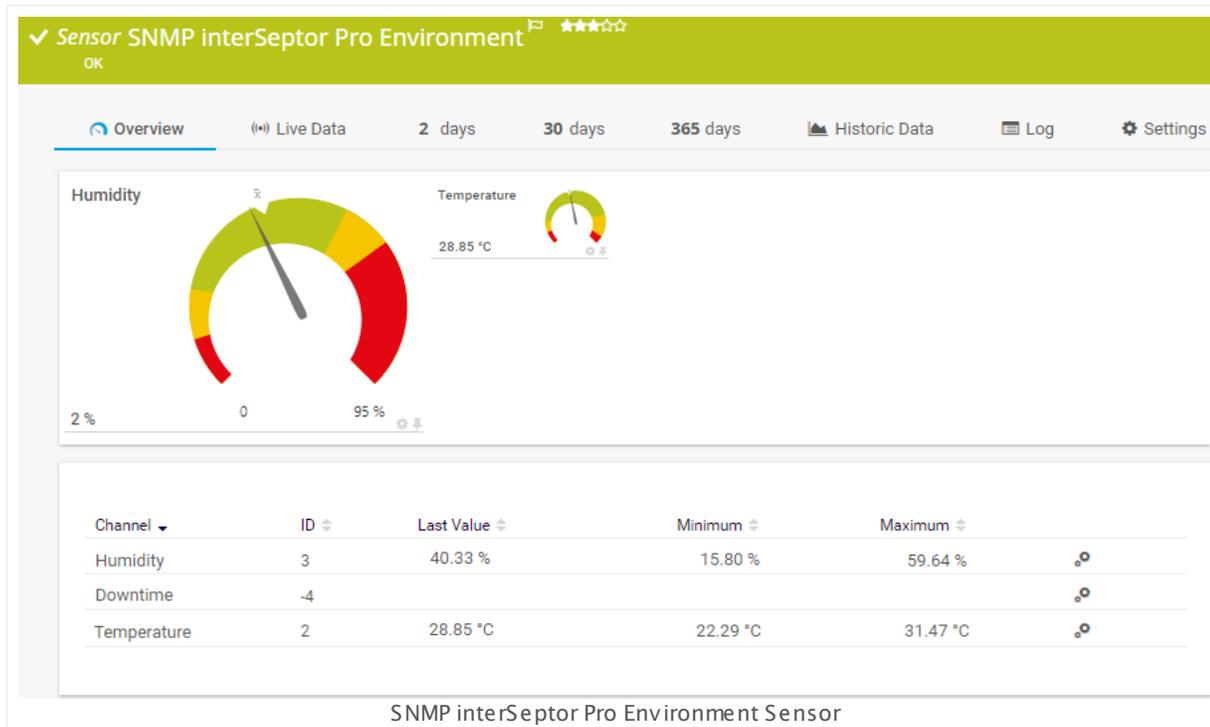
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.163 SNMP interSeptor Pro Environment Sensor

The SNMP interSeptor Pro Environment sensor queries data from a Jakarta interSeptor Pro environmental monitoring system via Simple Network Management Protocol (SNMP).

It can show the following as measured by the Jakarta interSeptor Pro device:

- Temperature
- Humidity



Sensor in Other Languages

Dutch: **SNMP interSeptor Pro Omgeving**, French: **Environnement interSeptor Pro SNMP**, German: **SNMP interSeptor Pro Umgebung**, Japanese: **SNMP InterSeptor Pro? ?**, Portuguese: **Ambiente do SNMP interSeptor Pro**, Russian: **Окружающая среда interSeptor Pro по SNMP**, Simplified Chinese: **SNMP interSeptor Pro? ?**, Spanish: **Entorno de interSeptor Pro de SNMP**

Remarks

- To monitor data of an interSeptor Pro device with this sensor, you have to add the IP address of your PRTG installation to **Access Control** in the interSeptor Pro control panel. Open the interSeptor Pro web interface, select **InterSeptor Pro Menu | System Configuration | Access Control**, and allow access for the IP address of PRTG.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the measuring points of interSeptor Pro device you want to monitor. PRTG will create one sensor for each measuring point you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

INTERSEPTOR ENVIRONMENT SPECIFIC

Measuring Point Select the measuring points you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

INTERSEPTOR ENVIRONMENT SPECIFIC

Name	<p>Shows information about the measurement that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Measuring Point	<p>Shows the measuring point that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p>

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

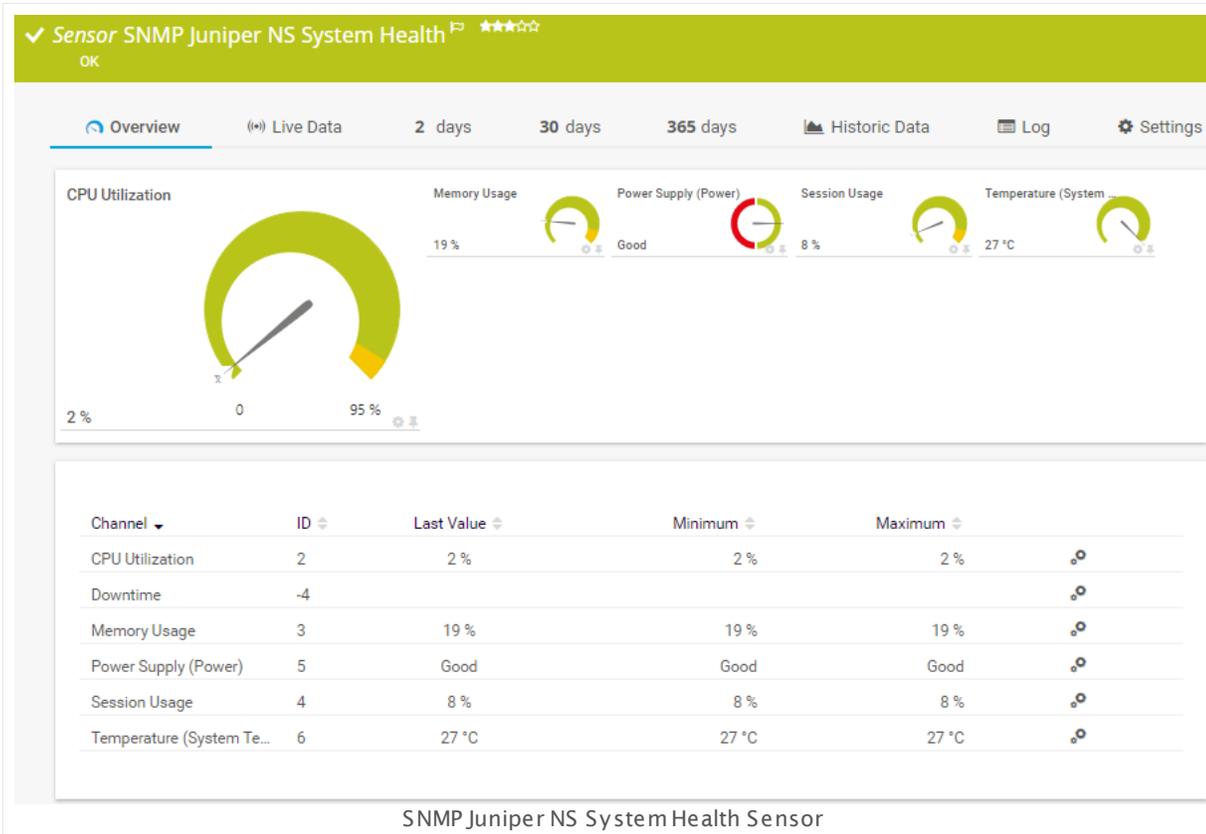
7.8.164 SNMP Juniper NS System Health Sensor

The SNMP Juniper NS System Health sensor monitors the system health of a Juniper NetScreen device using Simple Network Management Protocol (SNMP).

It can show the following:

- CPU utilization
- Fan status
- Power supply status
- System temperature
- Memory usage in percent
- Session usage in percent

These channels are created at run-time, depending on the available measurement components of your Juniper NetScreen device. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP Juniper NS systeemstatus**, French: **État du système SNMP Juniper NS**,
 German: **SNMP Juniper NS Systemzustand**, Japanese: **SNMP Juniper NS ? ? ? ? ? ? ? ,**

Portuguese: **Funcionamento do sistema Juniper NS SNMP**, Russian: **Работоспособность системы Juniper NS no SNMP**, Simplified Chinese: **SNMP Juniper NS ? ? ? ? ?**, Spanish: **Salud del sistema NS de Juniper SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰ from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

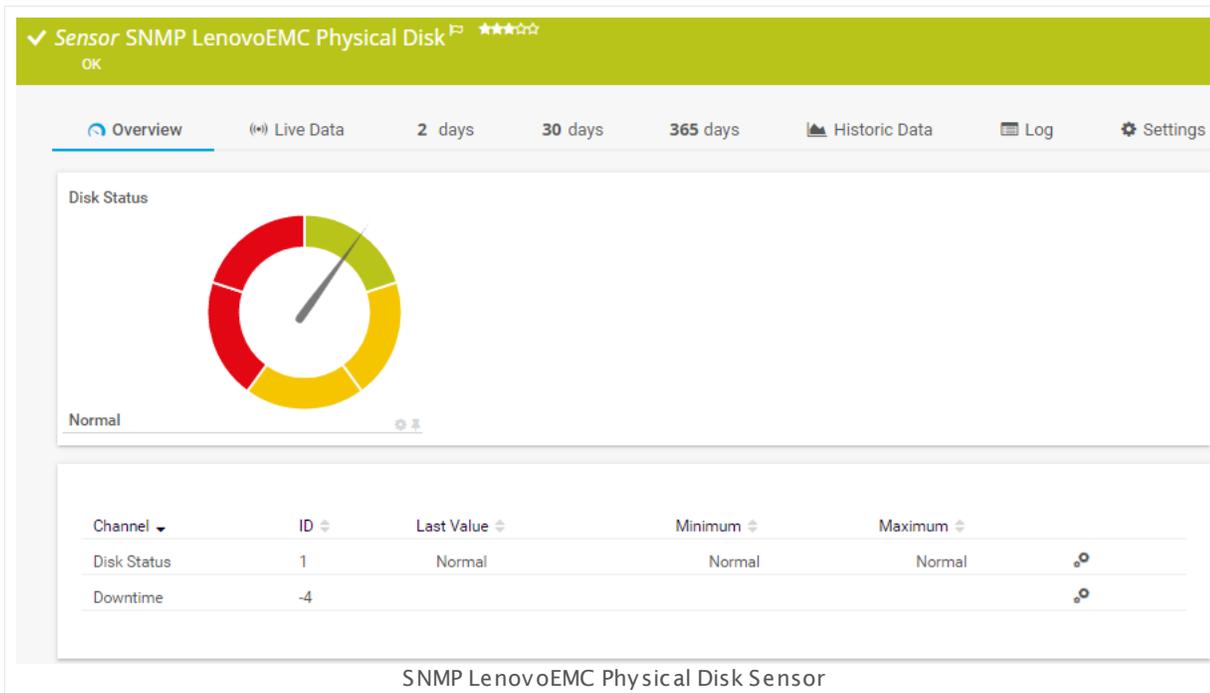
7.8.165 SNMP LenovoEMC Physical Disk Sensor

The SNMP Lenovo Physical Disk sensor monitors a physical disk in a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It shows the overall disk status.

States of the disk can be:

- **Normal** (sensor status **Up**),
- **Unknown** (sensor status **Warning**)
- **Foreign** (sensor status **Warning**)
- **Faulted** (sensor status **Down**)
- **Missing** (sensor status **Down**)



Sensor in Other Languages

Dutch: **SNMP LenovoEMC fysieke schijf**, French: **Disque physique SNMP LenovoEMC**, German: **SNMP LenovoEMC Physikalische Disk**, Japanese: **SNMP LenovoEMC ? ? ? ? ? ?**, Portuguese: **Disco físico LenovoEMC SNMP**, Russian: **Физический диск LenovoEMC по SNMP**, Simplified Chinese: **SNMP LenovoEMC ? ? ? ?**, Spanish: **Disco físico de LenovoEMC con SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the LenovoEMC NAS. PRTG creates one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

LENOVOEMC PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

LENOVOEMC NAS SETTINGS

Disk	Shows the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
165 SNMP LenovoEMC Physical Disk Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.166 SNMP LenovoEMC System Health Sensor

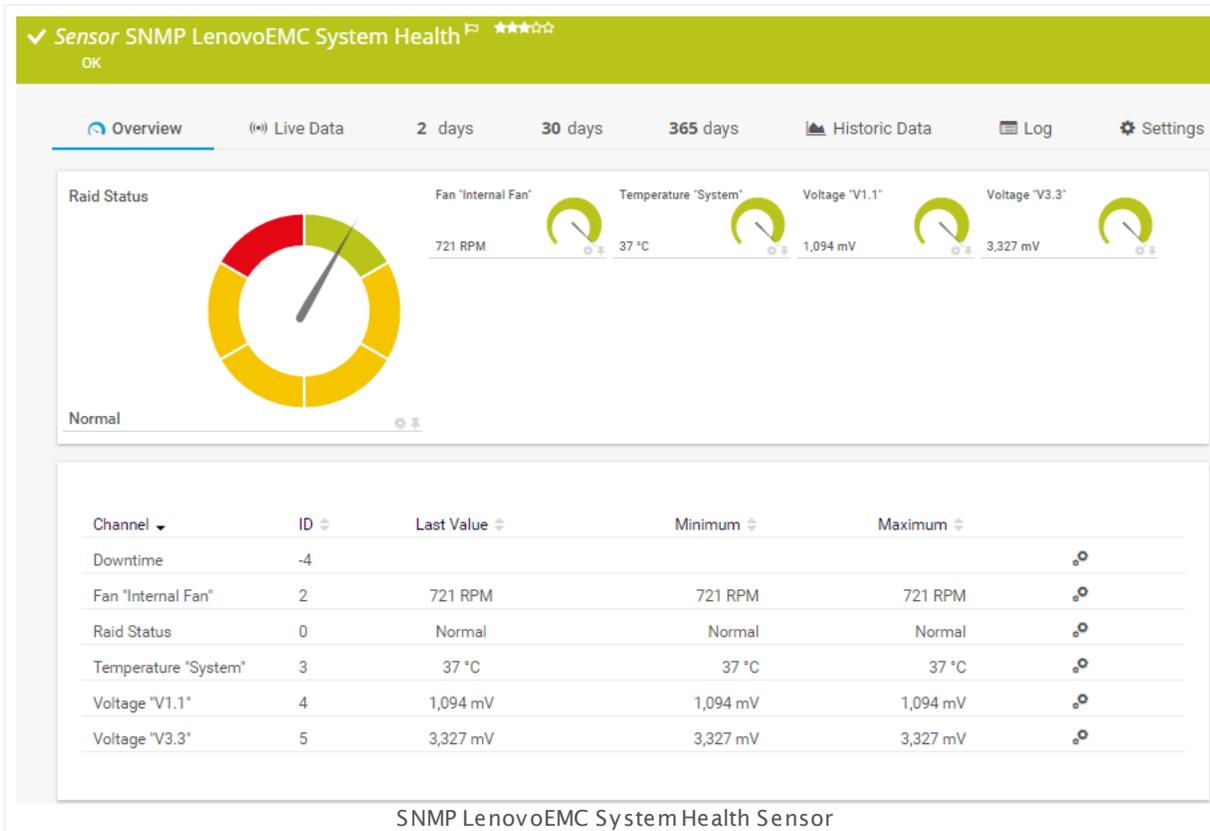
The SNMP LenovoEMC System Health sensor monitors the system health of a LenovoEMC Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It shows the overall status of the RAID.

[Sensor states](#) can be:

- **Normal** (sensor status **Up**)
- **Unknown** (sensor status **Warning**)
- **Rebuilding** (sensor status **Warning**)
- **Degraded** (sensor status **Warning**)
- **RebuildFS** (sensor status **Warning**)
- **Failed** (sensor status **Down**)

Furthermore, this sensor can show, for example, states of several fans, voltages, and temperatures. These channels are created at run-time depending on the available measurement components in the LenovoEMC NAS. Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP LenovoEMC System Status**, French: **État du système SNMP LenovoEMC**, German: **SNMP LenovoEMC Systemzustand**, Japanese: **SNMP LenovoEMC ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema LenovoEMC SNMP**, Russian: **Работоспособность системы LenovoEMC по SNMP**, Simplified Chinese: **SNMP LenovoEMC ? ? ? ? ? ? ?**, Spanish: **Estado del sistema de LenovoEMC del SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
- i** It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- i** You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
- i** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[3160] settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.167 SNMP Library Sensor

The SNMP Library sensor uses a compiled Management Information Base (MIB) library file to create sensors that monitor a device via Simple Network Management Protocol (SNMP). This approach provides custom monitoring beyond the standard SNMP sensors of PRTG.

The content of the MIB file will determine which data types are available for monitoring. When you create the sensor, it will provide a list of counters that came back from the target device based on checking every Object Identifier (OID) in the MIB. From this list, you can choose what you want to monitor.

The SNMP Library sensor will automatically create the following custom SNMP sensor types based on the data types available in the MIB:

- [SNMP Custom Advanced sensors](#)¹⁹⁸⁹ for all OIDs that return single values
- [SNMP Custom String sensors](#)¹⁹⁷⁰ for all OIDs that return string values
- [SNMP Custom Table sensors](#)¹⁹⁹² for all OIDs that return tables

 The SNMP Library sensor is not actually a sensor type and will not appear as running sensor. It is a sensor that uses the meta-scan facility of the PRTG probe to find or match OIDs from an MIB and eases the creation of custom sensors, because you do not have to enter the OIDs manually.

To monitor SNMP capable devices and add sensors using the SNMP Library sensor, download the manufacturer's MIB files for the target device, convert the MIB file to the Paessler **oidlib** format, and import it into PRTG. To make setting up your monitoring as convenient as possible, PRTG comes with pre-compiled **oidlib** library files that already contain the OIDs of SNMP counters for the most common devices in a network.

 For more details, see the Knowledge Base: [How do SNMP, MIBs and OIDs work?](#)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

167 SNMP Library Sensor



Sensor in Other Languages

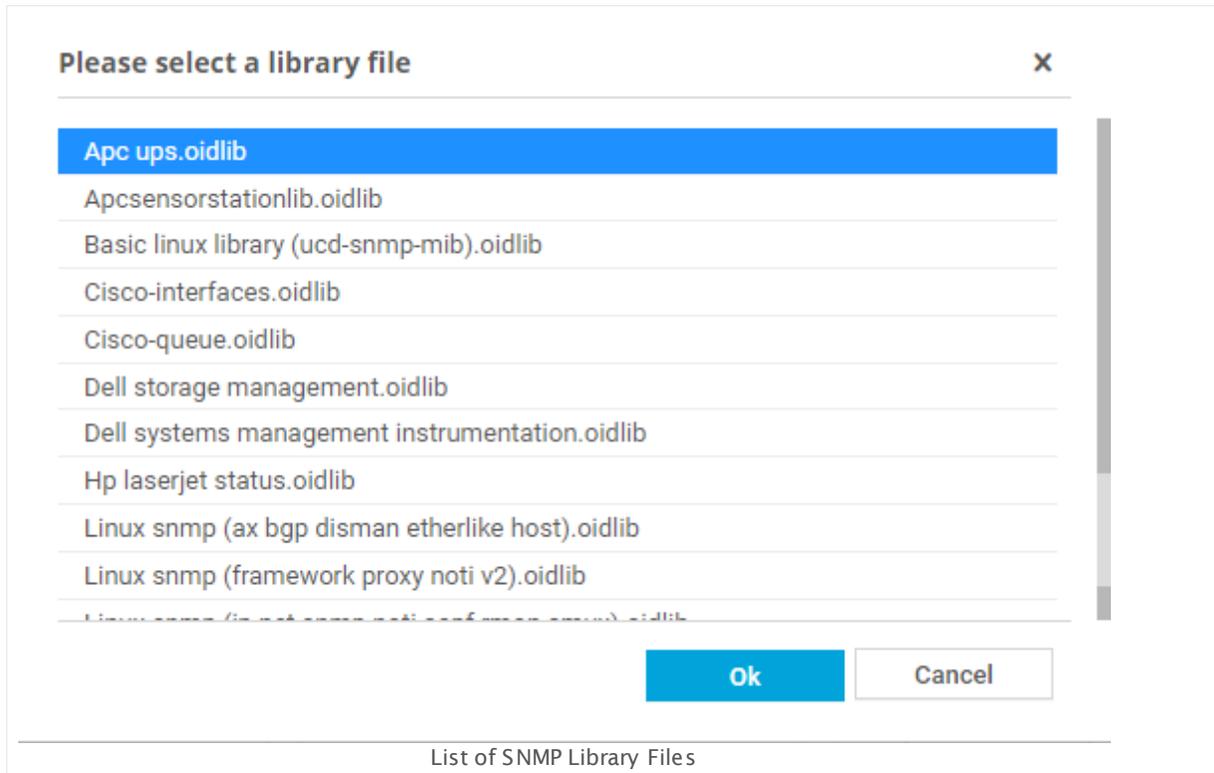
Dutch: **SNMP Bibliot heek**, French: **Bibliothèque SNMP**, German: **SNMP-Bibliot hek**, Japanese: **SNMP ? ? ? ? ?**, Portuguese: **Biblioteca SNMP**, Russian: **Библиотека SNMP**, Simplified Chinese: **SNMP ?**, Spanish: **Biblioteca SNMP**

Remarks

- Knowledge Base: [How do SNMP, MIBs and OIDs work?](#)
- Knowledge Base: [How can I import my MIB files into PRTG?](#)
- Knowledge Base: [Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) ³⁴⁸⁹.

Add Sensor

[Manually add](#)³²⁵ a new sensor to an SNMP device. From the **Add Sensor** dialog, select **SNMP Library** sensor. PRTG will show a list of **oidlib** files available on the system. This contains all library files stored at the `\snmplibs` folder of your PRTG server installation directory—both the ones delivered with PRTG and your own files.



The filenames on the list indicate the likely purpose. Select a name that appears appropriate for your device (for example, choose an MIB file that you imported before) and confirm via **OK**. Often, the **Paessler common oid library.oidlib** is a good start.

⚠ If the file does not fit to your device, this will result in the error message **the scan for available monitoring items has failed** on this device: **No such object (SNMP error # 222)**. If you see this message, click **Cancel** and try adding the sensor with another file.

The SNMP Library sensor takes a list of OIDs that you imported from an MIB file into an oidlib and tests the OIDs against a device to find the OIDs the device supports. This discovery process is the **meta-scan**.

✓ If counters were found for your device, the sensor settings will open with a list of available monitoring items for you to select from. PRTG sorts the list in advance to make the related values sequential in the list.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 167 SNMP Library Sensor

SNMP Library Specific

Library ⓘ C:\Program Files (x86)\PRTG Network Monitor\snmplibs\Linux SNMP (Framework Proxy Noti v2).oidlib

Library-OIDs Search... 🔍

<input type="checkbox"/>	⇅ MIB Module	⇅ Category	⇅ Name
<input type="checkbox"/>	SNMP-MPD-MIB	snmpmpdstats	snmp unknown security models
<input type="checkbox"/>	SNMP-MPD-MIB	snmpmpdstats	snmp unknown pdu handlers
<input type="checkbox"/>	SNMP-MPD-MIB	snmpmpdstats	snmp invalid msgs
<input type="checkbox"/>	SNMPv2-MIB	sysor: 1	sysorup time
<input type="checkbox"/>	SNMPv2-MIB	sysor: 10	sysorup time
<input type="checkbox"/>	SNMPv2-MIB	sysor: 2	sysorup time

This field is required.

If Value Changes ⓘ Ignore changes
 Trigger 'change' notification

List of SNMP Single Values: Sorted by MIB, Category, Name

SNMP Library Specific

Library ⓘ C:\Program Files (x86)\PRTG Network Monitor\snmplibs\Linux SNMP (Source TCP UCD UDP).oidlib

Library-OIDs Search... 🔍

<input type="checkbox"/>	⇅ MIB Module	⇅ Category	⇅ Name
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 19	diskioindex
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 2	diskiowrites
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 2	diskioreads
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 2	diskionwrittenx
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 2	diskionwritten
<input type="checkbox"/>	UCD-DISKIO-MIB	diskio: 2	diskioerrors

This field is required.

If Value Changes ⓘ Ignore changes
 Trigger 'change' notification

List of SNMP Table Values: Sorted by MIB, Category (Table Name/OID), Row, Name

The list of SNMP table values presents row values sequentially and makes it easier for you to select the values you are interested in.

You can also use the search function to find the desired group or category. The search matches individual strings so if your string has a space in it, enclose the search string in quotes.

- ✔ Select the desired counters and click **Save**. PRTG will now create sensors based on the OID types of the selected entries.
 - For selected SNMP single values, PRTG will create [SNMP Custom Advanced sensors](#) with up to 10 channels for 10 OIDs each. For example, 22 selected single values will result in 3 sensors: 2 sensors with 10 channels and 1 sensor with 2 channels.
 - If you select OIDs that return string values, PRTG will create one [SNMP Custom String sensor](#) for each selected entry that returns a string value.
 - For selected SNMP table entries, PRTG will create [SNMP Custom Table sensors](#) with up to 10 channels for 10 columns per row.
- ❗ Once a custom SNMP sensor is created, you can [create a device template](#) from it and prepare it for distribution. For example, you can refine the template with better name templates.

Default OIDLIB Files Overview

The following files are included in PRTG and allow the extension of your SNMP monitoring to many devices. Please be aware that not all devices and/or parameters may be supported by the libraries.

- **APC UPS.oidlib**
Can be used to monitor uninterruptible power supplies (UPS) from APC American Power Conversion Corp.
- **APCSensorstationlib.oidlib**
Can be used to monitor alarm status, communication status, humidity, and temperature as shown by an APC sensor station.
- **Basic Linux Library (UCD-SNMP-MIB).oidlib**
Can be used to monitor basic system parameters on Linux systems, such as memory, disk and swap, CPU, etc.
- **cisco-interfaces.oidlib**
Can be used to monitor Cisco specific parameters, for example, the number of present network interfaces on a system, several states of an interface (admin, oper, speed, type, errors, discards, etc.), and more.
- **cisco-queue.oidlib**
Can be used to monitor queues on a Cisco interface, for example, queue depth and its maximum, discarded messages from the queue, the number of the queue within the queue set, etc.
- **Dell Storage Management.oidlib**
Can be used to monitor Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, etc.

- **Dell Systems Management Instrumentation.oidlib**
Can be used to monitor the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, Bios, BMC, chassis, COO, cooling, event log, firmware, IDE, keyboard, memory, port, network, processor, SCSI, system, temperature, USB, UUID, etc.
- **HP LaserJet Status.oidlib**
Can be used to monitor toner, paper, and jam status of an HP LaserJet printer.
- **Linux SNMP (AX BGP DisMan EtherLike Host).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Framework Proxy Not i v2).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (IP Net SNMP Not i OSPF RMON SMUX).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Source TCP UCD UDP).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Paessler Common OID Library.oidlib**
Can be used to monitor many common hardware devices. It is used for several sensors and is encrypted.
- **SNMP Informant std.oidlib**
Can be used to monitor logical disks, processor, memory, and network interface on Windows systems.

Import MIB Files

Additionally, you can create your own **oidlib** files by importing your device manufacturers' MIB files with the free tool Paessler **MIB Importer**. Simply convert your **mib** files and save the resulting **oidlib** files to the `\snmplibs` subfolder of your PRTG program directory.

 For details about directory paths, see section [Data Storage](#) .

 For more information about the **MIB Importer** and to download this tool, see the Knowledge Base: [How can I import my MIB files into PRTG?](#)

 If your imported **oidlib** file contains [lookups](#)  (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. Add an SNMP Library sensor using this **oidlib**. PRTG will then create a lookup definition file using the **lookupname** of the chosen library as **id** parameter.

Important: The lookups will be added without state definitions, so the sensor will show a **Warning status** ^[195] by default! You have to edit the corresponding lookup files to get reliable alarms. Please override the lookup definition with your own custom lookup as described in section [Define Lookups—Customizing Lookups](#) ^[3698].

 PRTG hosted by Paessler does not support the import of MIB files. You can use the SNMP Library sensor only with the default **oidlib** files in PRTG hosted by Paessler.

SNMP Library Sensor—Add Sensor Settings

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP LIBRARY SPECIFIC

Library	Shows the path to the oidlib file selected before. This setting is shown for your information only and cannot be changed here.
Library-OIDs	<p>Select the parameters of the device you want to monitor. A list specific to your setup is shown. It contains all counters found in the chosen library that match your device.</p> <p>Choose one or more items by adding a check mark in front of the respective line. You can also select and deselect all items by using the check box in the table head. Use the search box to narrow down to your desired items.</p> <p>Depending on the kind of the chosen entries, PRTG will create the following sensor types:</p> <ul style="list-style-type: none"> ▪ SNMP Custom Advanced sensor ^[1989]: one sensor for every 10 single values ▪ SNMP Custom String sensor ^[1970]: one sensor for each selected entry that returns a string value ▪ SNMP Custom Table sensor ^[1992]: one sensor for each selected table row with up to 10 channels representing values in the columns of the same row

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) ^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

 The available sensor settings depend on the sensor type that the SNMP Library sensor has created. For details about settings, see the manual sections of these sensor types:

- [SNMP Custom Advanced sensor](#)^[1962]
- [SNMP Custom String sensor](#)^[1972]
- [SNMP Custom Table sensor](#)^[1996]

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How do SNMP, MIBs and OIDs work?

- <https://kb.paessler.com/en/topic/653>

Knowledge Base: How can I import my MIB files into PRTG?

- <https://kb.paessler.com/en/topic/733>

Knowledge Base: Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?

- <https://kb.paessler.com/en/topic/65638>

Knowledge Base: How can I monitor EMC Isilon storage systems with PRTG?

- <https://kb.paessler.com/en/topic/71413>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

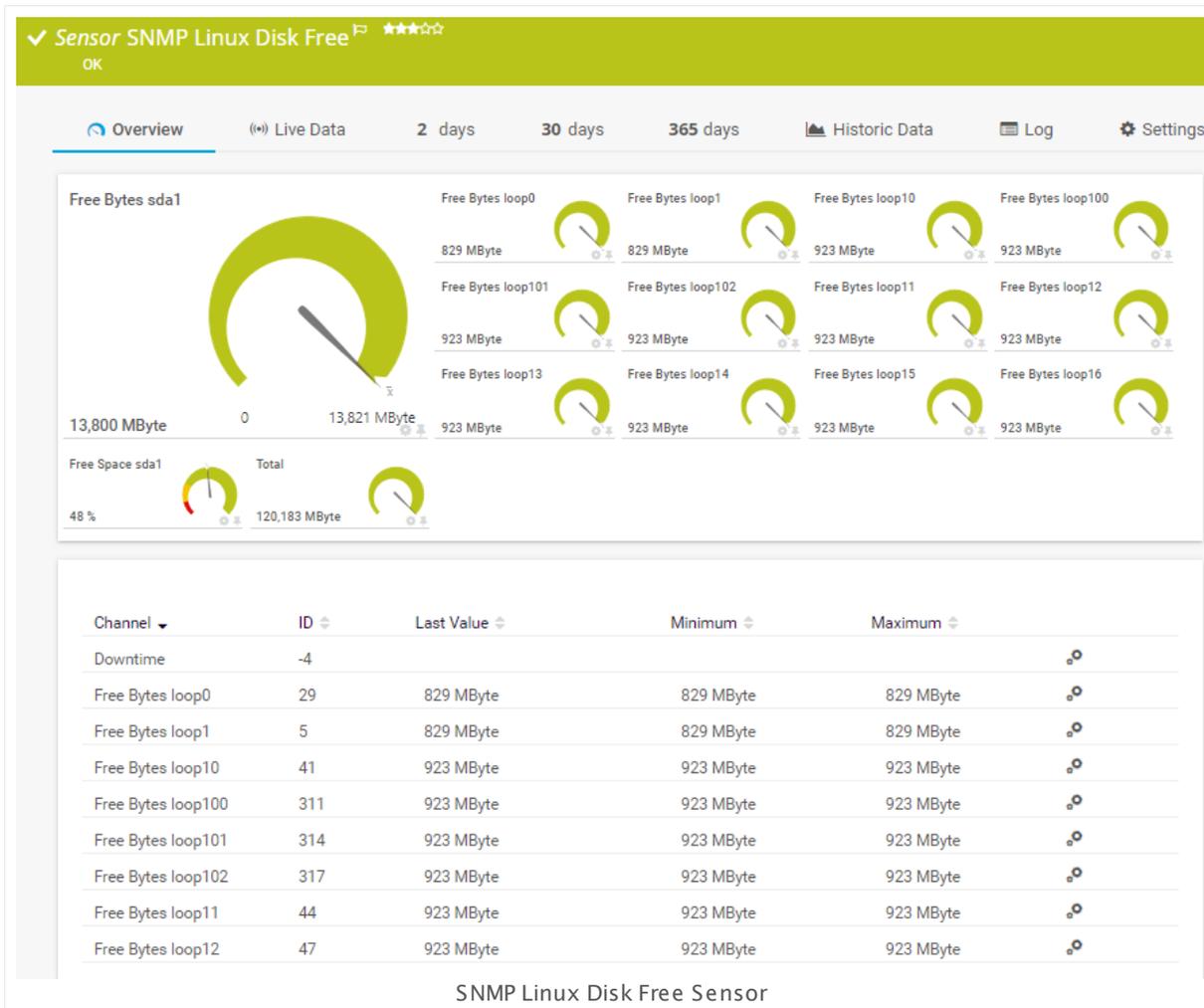
7.8.168 SNMP Linux Disk Free Sensor

The SNMP Linux Disk Free sensor monitors free space on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Free total disk space in bytes
- Free space in bytes for every mounted partition
- Free space in percent for every mounted partition
- Free inodes in percent for every mounted partition

 The free space returned by this sensor type shows the disk space that is not yet used. Not all of this space may be available for use, as a part of this space can be reserved by the system, for example, for redundancy purposes. For details, see the Knowledge Base: [Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?](#)



Sensor in Other Languages

Dutch: **SNMP Linux vrije schijf ruimte**, French: **Espace disque libre SNMP Linux**, German: **SNMP Linux Datenträgerspeicher**, Japanese: **SNMP Linux** ? ? ? ? ? ? ? , Portuguese: **Disco livre Linux SNMP**, Russian: **Свободное пространство диска в Linux по SNMP**, Simplified Chinese: **SNMP Linux** ? ? ? ? ? ? ? , Spanish: **SNMP disco libre Linux**

Remarks

- Knowledge Base: [Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?](#)
- Knowledge Base: [Checklist: Setting up SNMP on Linux](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
- i** It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down status**^[195], depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, please use the limit settings in the [Sensor Channels Settings](#)^[2160].

i All limits that you define here are valid in addition to the limits defined in the particular **Channel** settings! The limits are valid simultaneously, so the first limit that is breached applies.

- Percentage Limit Check** Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between:
- **Only use the limits in the settings of the percentage channels:** Do not define sensor limits that are valid for all percentage channels. The sensor only uses limits that you define in the settings of the particular "free space in percent" channels to determine the status.
 - **Use the limits of both the sensor and the channel settings:** Define limits for the sensor that are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

SET LIMITS CHECKED AGAINST ALL DISKS

Upper Error Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Warning Limit This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Warning** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Error Limit This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Down** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Size Limit Check Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between:

SET LIMITS CHECKED AGAINST ALL DISKS

- **Only use the limits in the settings of the byte size channels:**
Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.
- **Use the limits of both the sensor and the channel settings:**
Define limits for the sensor that are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will switch to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Warning Limit

This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Lower Error Limit This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Alarm on Missing/Removed Disk If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between:

- **Deactivate alarm (default):** Select this option if you do not want an alarm for a removed disk.
- **Activate alarm:** Select this option if you want to be alerted if a monitored disk is removed.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <https://kb.paessler.com/en/topic/43183>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Checklist: Setting up SNMP on Linux

- <https://kb.paessler.com/en/topic/5353>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

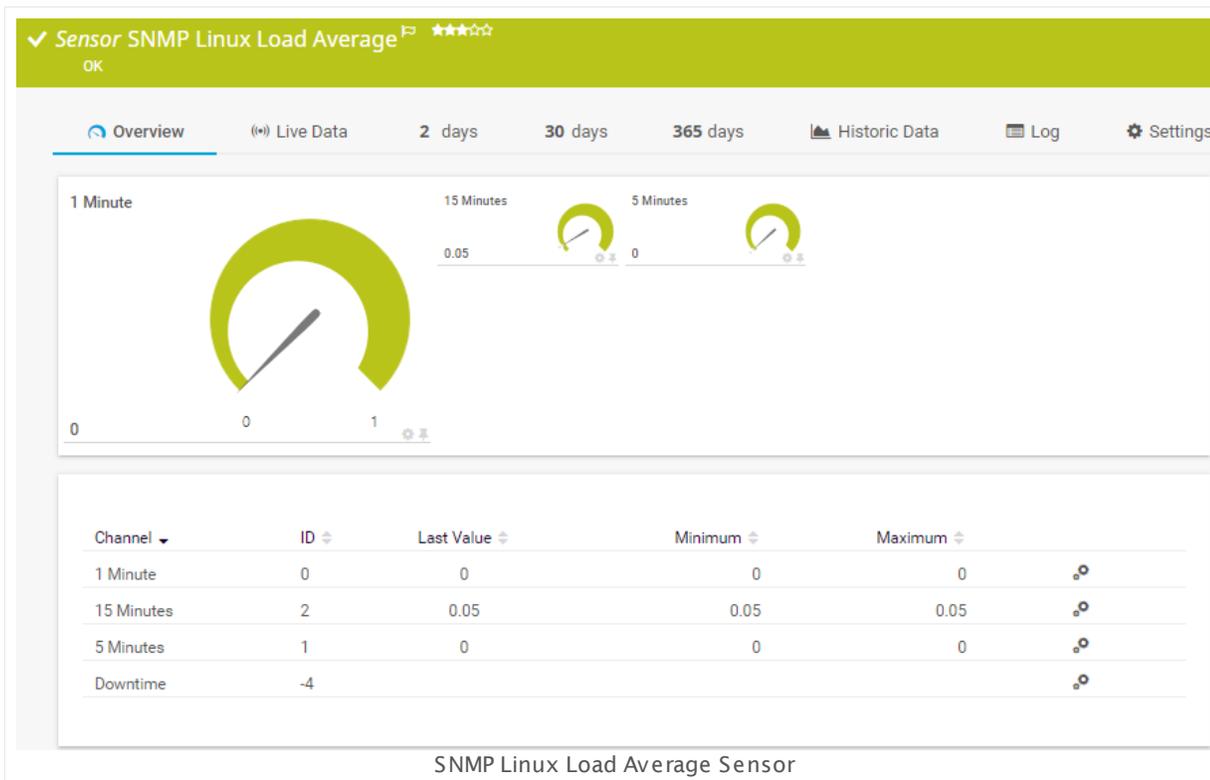
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.169 SNMP Linux Load Average Sensor

The SNMP Linux Load Average sensor monitors the system load average of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Average system load within a 1-minute interval
- Average system load within a 5-minute interval
- Average system load within a 15-minute interval



Sensor in Other Languages

Dutch: **SNMP Linux Gemiddelde belasting**, French: **Moyenne de la charge Linux SNMP**, German: **SNMP Linux Durchschnittl. Last**, Japanese: **SNMP Linux 平均値**, Portuguese: **Carga média em Linux SNMP**, Russian: **Средняя загрузка Linux по SNMP**, Simplified Chinese: **SNMP Linux 平均值**, Spanish: **SNMP carga promedio Linux**

Remarks

- Knowledge Base: [Checklist: Setting up SNMP on Linux](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Checklist: Setting up SNMP on Linux

- <https://kb.paessler.com/en/topic/5353>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
169 SNMP Linux Load Average Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

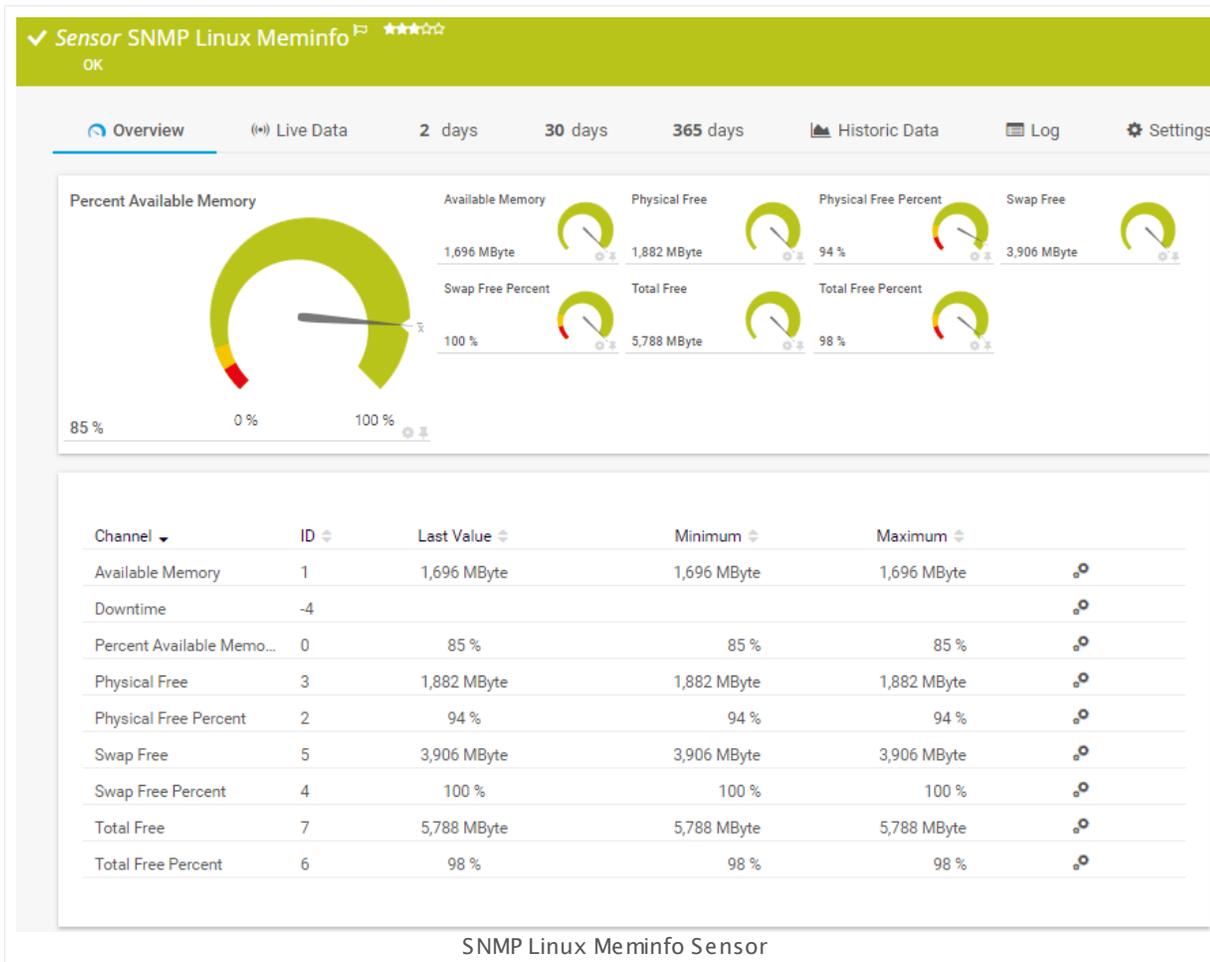
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.170 SNMP Linux Meminfo Sensor

The SNMP Linux Meminfo sensor monitors the memory usage of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following :

- Available memory in absolute and percentage values
- Used physical memory (free memory plus buffer plus cache) in percent
- Free physical memory (free memory plus buffer plus cache) in bytes
- Used swap memory in percent
- Free swap memory in bytes
- Used memory on the whole system (physical memory plus swap) in percent
- Free memory on the whole system (physical memory plus swap) in bytes



Sensor in Other Languages

Dutch: **SNMP Linux meminfo**, French: **Info sur la mémoire SNMP Linux**, German: **SNMP Linux**

Speicherinfo, Japanese: **SNMP Linux** ? ? ? ? ? , Portuguese: **Linux Meminfo SNMP**, Russian: **Linux Meminfo no SNMP**, Simplified Chinese: **SNMP Linux** ? ? ? ? ? , Spanish: **SNMP información de memoria Linux**

Remarks

- Knowledge Base: [Checklist: Setting up SNMP on Linux](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited ^[140] from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[336] on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
-  Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
-  If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <ul style="list-style-type: none"> ❗ To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Checklist: Setting up SNMP on Linux

- <https://kb.paessler.com/en/topic/5353>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

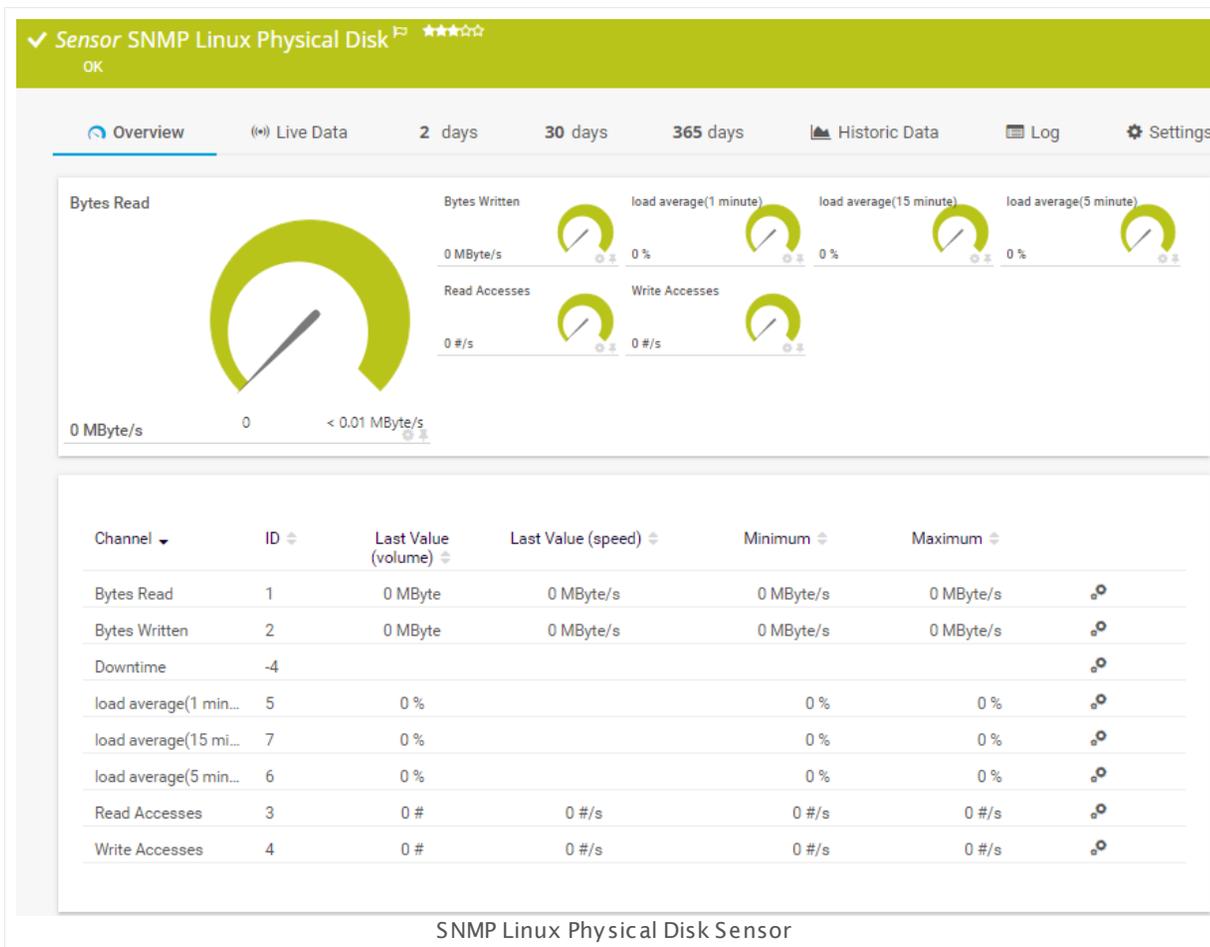
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.171 SNMP Linux Physical Disk Sensor

The SNMP Linux Physical Disk sensor monitors input/output (I/O) on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Read bytes per second
- Written bytes per second
- Number of read accesses per second
- Number of write accesses per second



Sensor in Other Languages

Dutch: **SNMP Linux Fysieke Schijf**, French: **Disque physique Linux SNMP**, German: **SNMP Linux Physikalischer Datenträger**, Japanese: **SNMP Linux** , Portuguese: **Disco físico Linux SNMP**, Russian: **Физический диск Linux по SNMP**, Simplified Chinese: **SNMP Linux** , Spanish: **Disco físico de Linux con SNMP**

Remarks

- Knowledge Base: [Checklist: Setting up SNMP on Linux](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks of the Linux/Unix system you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
-------------	--

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

PHYSICAL DISK SETTINGS

Disk	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value.
Bitmask	It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Checklist: Setting up SNMP on Linux

- <https://kb.paessler.com/en/topic/5353>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

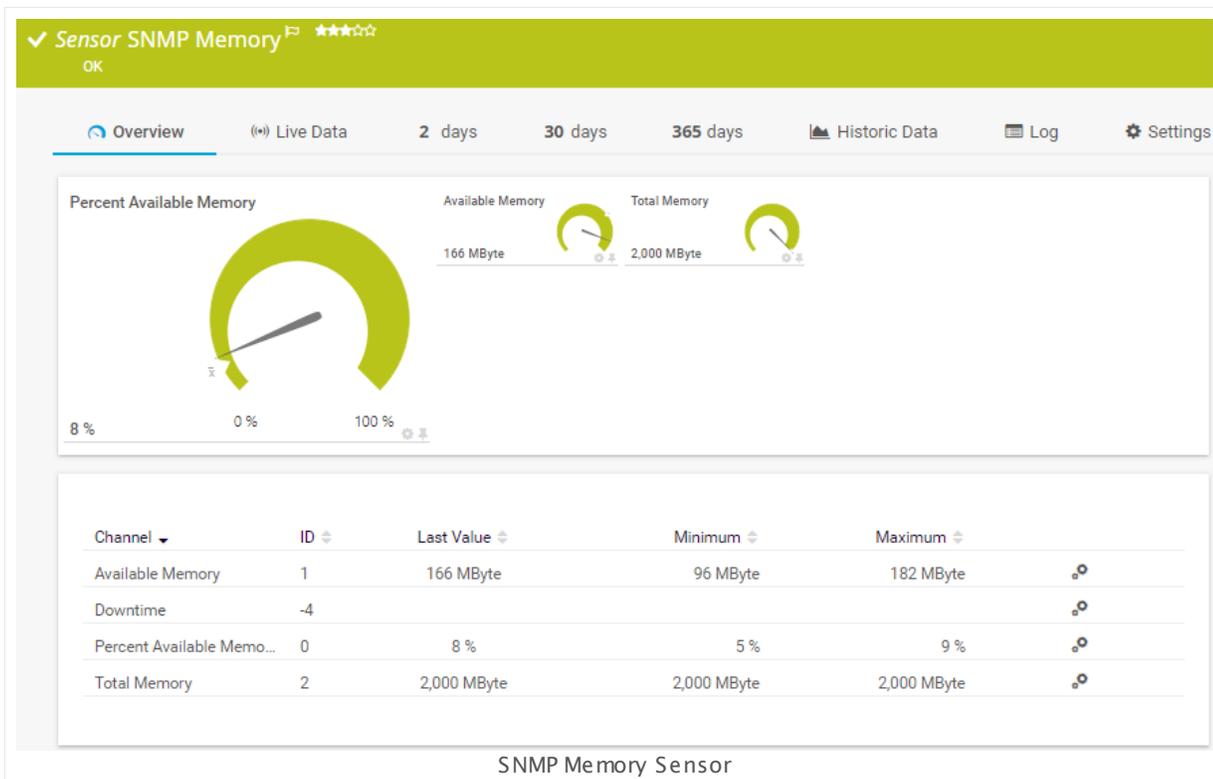
7.8.172 SNMP Memory Sensor

The SNMP Memory sensor monitors the memory usage of a system via Simple Network Management Protocol (SNMP).

It can show the following:

- Available memory in bytes
- Available memory in percent
- Total memory

 This sensor uses more generic Object Identifier (OID) values compared to the [SNMP Linux Meminfo Sensor](#).



Sensor in Other Languages

Dutch: **SNMP Geheugen**, French: **Mémoire SNMP**, German: **SNMP Speicher**, Japanese: **SNMP ? ? ?**, Portuguese: **Memória SNMP**, Russian: **Память по SNMP**, Simplified Chinese: **SNMP ? ?**, Spanish: **SNMP Memoria**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the memory types you want to monitor. PRTG will create one sensor for each memory type you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

MEMORY SETTINGS

Memory Select one or more memory types you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

MEMORY SETTINGS

Memory	Shows the type of the memory that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
--------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

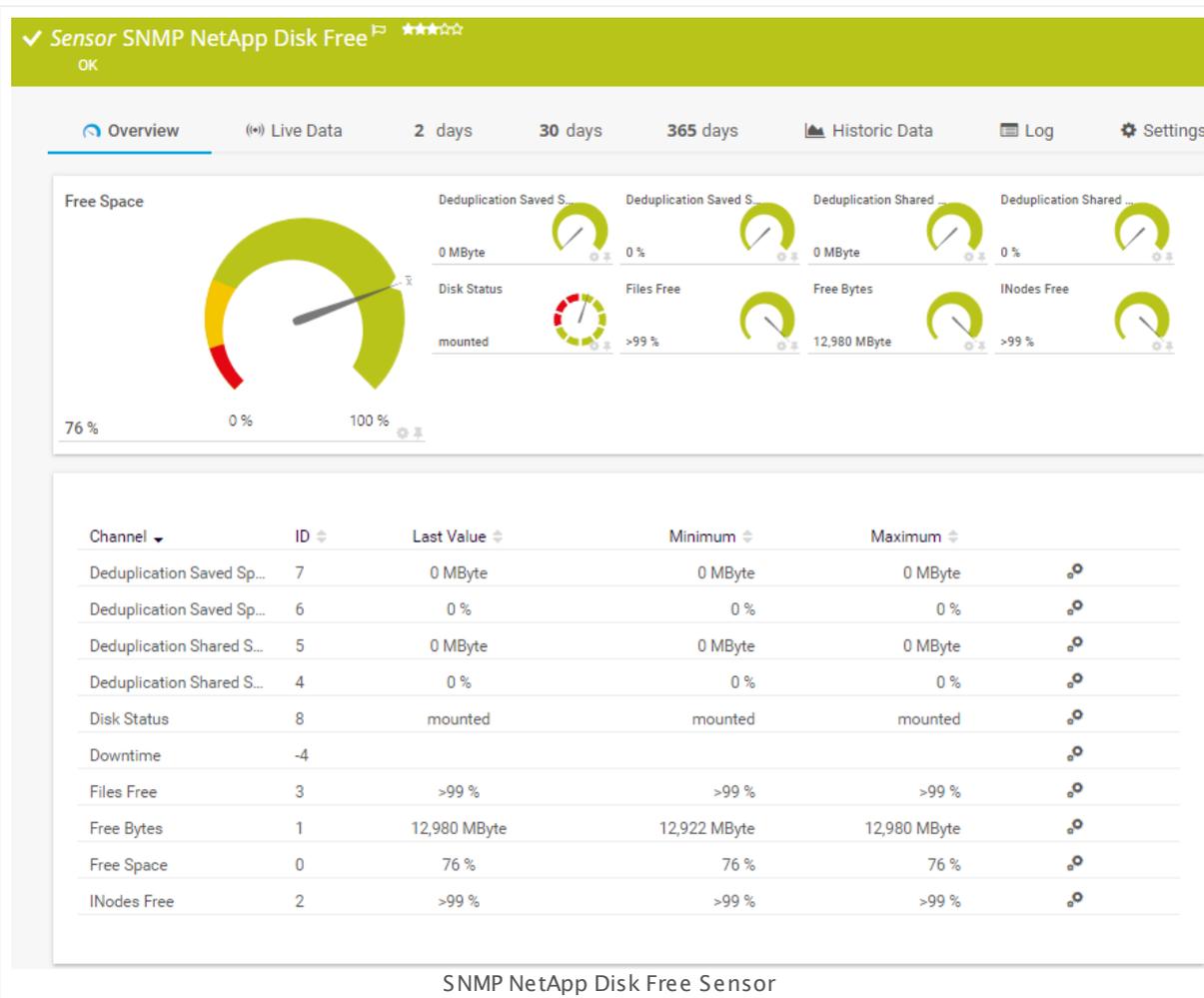
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.173 SNMP NetApp Disk Free Sensor

The SNMP NetApp Disk Free sensor monitors free space on disks of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in bytes and percent
- Deduplication saved space in bytes and percent
- Deduplication shared space in bytes and percent
- Disk free status
- Free files in percent
- Free INodes in percent



Sensor in Other Languages

Dutch: **SNMP NetApp Schijf Vrije Ruimte**, French: **Espace disque libre NetApp SNMP**,

German: **SNMP NetApp-Datenträgerspeicher**, Japanese: **SNMP NetApp ? ? ? ? ? ?** ,
Portuguese: **Disco livre SNMP NetApp**, Russian: **Свободное пространство диска NetApp по SNMP**,
Simplified Chinese: **SNMP NetApp ? ? ? ? ? ?** , Spanish: **SNMP Disco libre NetApp**

Remarks

- Knowledge Base: [How can I monitor capacity and used disk space on a NetApp?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk on the NetApp you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP DISK FREE SETTINGS

File System	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP DISK FREE SETTINGS

File System	Shows the name of the disk that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Virtual Disk	Shows the name of the virtual disk that this sensor is monitoring (if applicable). Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I monitor capacity and used disk space on a NetApp?

- <https://kb.paessler.com/en/topic/61231>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.174 SNMP NetApp Enclosure Sensor

The SNMP NetApp Enclosure sensor monitors the power supply and cooling of an enclosure that is part of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following, depending on the measurements you choose:

- Temperatures
- Rotations per minute (RPM) of fans and the number of failed fans
- Voltages in mV, the number of broken electronic parts, and the number of broken power supplies
- Currents in mA

✓ Sensor SNMP NetApp Enclosure ☆☆☆☆

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Voltage 1



5.070 mV

Broken electronic parts

0 #

Broken power supplies

0 #

Voltage 2

12.220 mV

Voltage 3

5.110 mV

Voltage 4

12.220 mV

Voltage 5

5.070 mV

Voltage 6

12.220 mV

Voltage 7

5.070 mV

Voltage 8

12.220 mV

Voltage 1

5.070 mV

Channel	ID	Last Value	Minimum	Maximum	
Broken electronic pa...	11	0 #	0 #	0 #	
Broken power suppli...	10	0 #	0 #	0 #	
Voltage 2	3	12.220 mV	-138.200 mV	12.340 mV	
Voltage 3	4	5.110 mV	-2.550 mV	5.150 mV	
Downtime	-4				
Voltage 4	5	12.220 mV	-148.440 mV	12.300 mV	
Voltage 5	6	5.070 mV	-12.790 mV	5.070 mV	
Voltage 6	7	12.220 mV	-148.440 mV	12.300 mV	
Voltage 7	8	5.070 mV	-12.790 mV	5.150 mV	
Voltage 8	9	12.220 mV	-148.440 mV	12.340 mV	
Voltage 1	2	5.070 mV	-12.790 mV	5.110 mV	

SNMP NetApp Enclosure Sensor

Sensor in Other Languages

Dutch: **SNMP NetApp Behuizing**, French: **Baie NetApp SNMP**, German: **SNMP NetApp Enclosure**, Japanese: **SNMP NetApp** ? ? ? ? ? ? ? , Portuguese: **Gabinete SNMP NetApp**, Russian: **Kopnye NetApp no SNMP**, Simplified Chinese: **SNMP NetApp** ? ? , Spanish: **SNMP NetApp**

Enclosure

Remarks

- This sensor type only supports NetApp versions up to 8.2.
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)³¹⁶⁰.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the power supply and cooling measurements of an enclosure on a NetApp you want to monitor. PRTG will create one sensor for each enclosure/measurement combination you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP ENCLOSURE SETTINGS

Enclosure	Select the enclosures with the measurement you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-----------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP ENCLOSURE SETTINGS

Enclosure	Shows the identifier of the enclosure that this sensor is monitoring. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Measurement	Shows the monitored measurement. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

NETAPP SPECIFIC

N/A Measurements

Define the sensor behavior if the requested NetApp value is not available (N/A values). Choose between:

- **Interpret as error (default):** Choose this option to set the sensor to a **Down status** if a measurement is not available. We recommend that you use this setting to not miss any hardware errors.
- **Interpret as valid:** Choose this option to handle unavailable measurements as valid sensor results to keep the sensor in **Up status**. This might be useful, for example, if a hardware sensor on the NetApp is disabled for some reason but actually there is no hardware error. If the NetApp returns an N/A measurement, the sensor will interpret this as 0.

 We recommend that you use the lookup file **prtg.standardlookups.netapp.notavailable.ovl** for channels with unavailable measurements if you choose this option. This will replace 0 with the message **Not Available**. Open the **Sensor Channels Settings** of the affected channel(s) and choose this file in section **Value Lookup**. For details, see section **Define Lookups**.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the **Sensor Channels Settings** settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

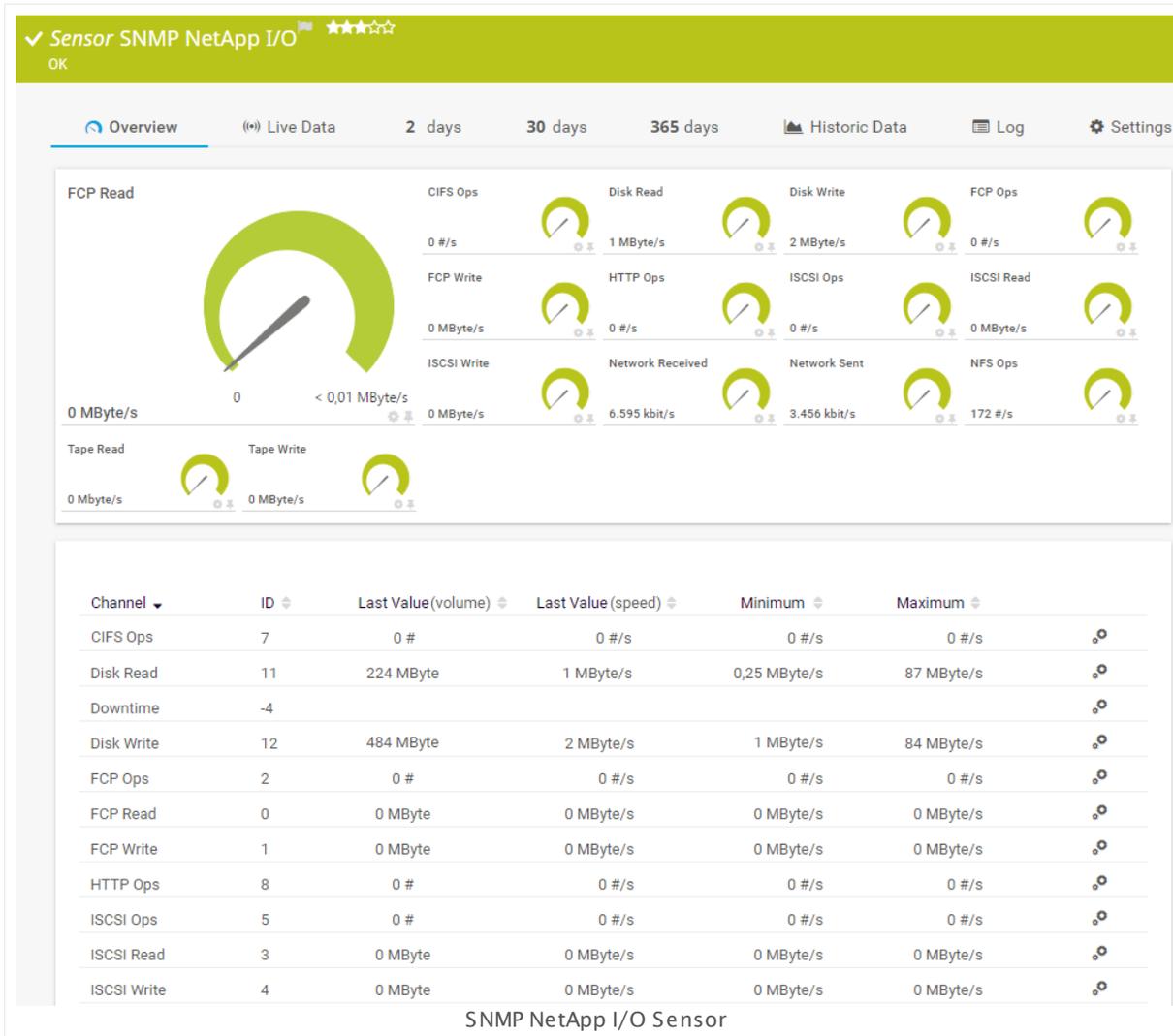
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.175 SNMP NetApp I/O Sensor

The SNMP NetApp I/O sensor monitors input/output operations (IOPS) on a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- FCP read speed
- CIFS operations per second
- Disk read speed
- Disk write speed
- FCP operations per second
- FCP read speed
- FCP write speed
- HTTP operations per second
- iSCSI operations per second
- iSCSI read speed
- iSCSI write speed
- Network received bytes
- Network sent bytes
- NFS operations per second
- Tape read speed
- Tape write speed



Sensor in Other Languages

Dutch: **SNMP NetApp I/O**, French: **NetApp SNMP E/S**, German: **SNMP NetApp E/A**, Japanese: **SNMP NetApp I/O**, Portuguese: **E/S SNMP Net App**, Russian: **Ввод-вывод NetApp по SNMP**, Simplified Chinese: **SNMP NetApp I/O**, Spanish: **SNMP NetApp I/O**

Remarks

- This sensor type only supports NetApp versions up to 8.2.
- If you use NetApp cDOT 8.3 or NetApp ONTAP 9.0 or later, we recommend that you use the [NetApp I/O sensor](#) ¹³¹¹ instead.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) ³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

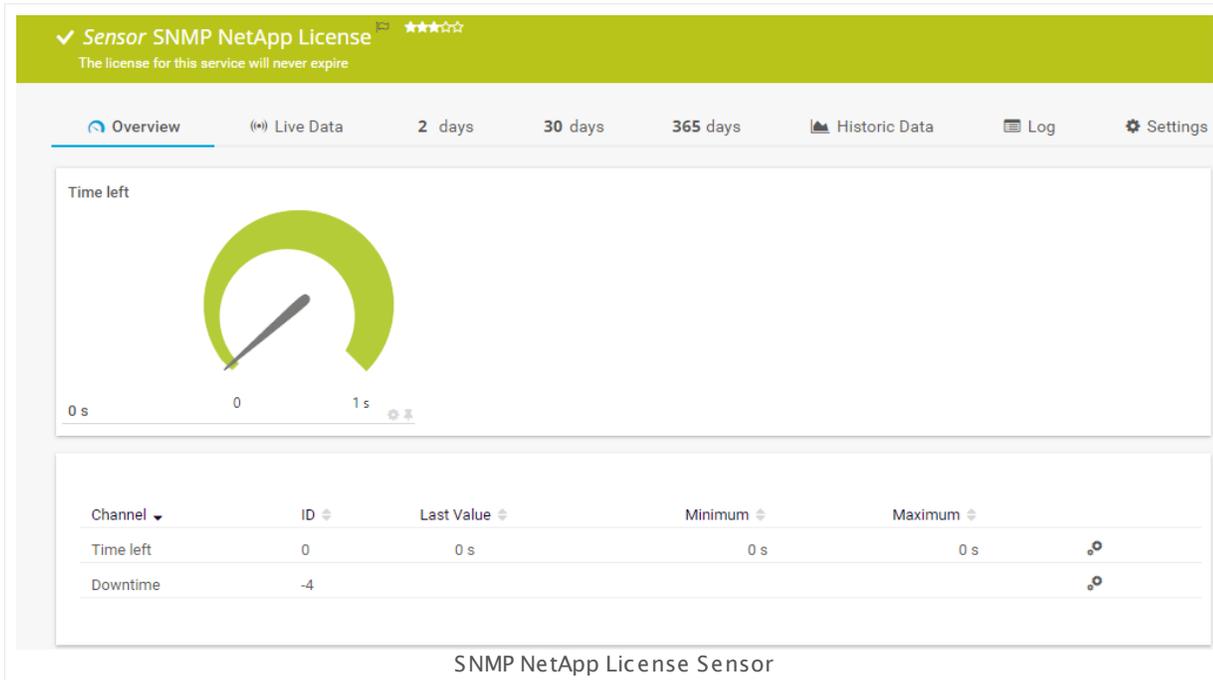
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.176 SNMP NetApp License Sensor

The SNMP NetApp License sensor monitors the licenses for the services of a NetApp storage system via Simple Network Management Protocol (SNMP).

- It shows how much time is left until the license for a service expires. This can help you detect when a NetApp license is going to expire.



Sensor in Other Languages

Dutch: **SNMP NetApp licentie**, French: **Licence Net App SNMP**, German: **SNMP Net App Lizenz**, Japanese: **SNMP NetApp** ? ? ? ? ? , Portuguese: **Licença SNMP Net App**, Russian: **Лицензия NetApp по SNMP**, Simplified Chinese: **SNMP NetApp** ? ? ? , Spanish: **SNMP Licencia Net App**

Remarks

- This sensor type only supports NetApp versions up to 8.2.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) ³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the NetApp license you want to monitor. PRTG will create one sensor for each license you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP LICENSE SETTINGS

License for Service Select the licenses you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) [402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) [181], as well as in [alarms](#) [219], [logs](#) [228], [notifications](#) [3216], [reports](#) [3252], [maps](#) [3276], [libraries](#) [3235], and [tickets](#) [230].

Parent Tags Shows [Tags](#) [139] that this sensor [inherits](#) [140] from its [parent device, group, and probe](#) [133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) [139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) [140] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP LICENSE SETTINGS

License for Service Shows the name of the service whose license this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

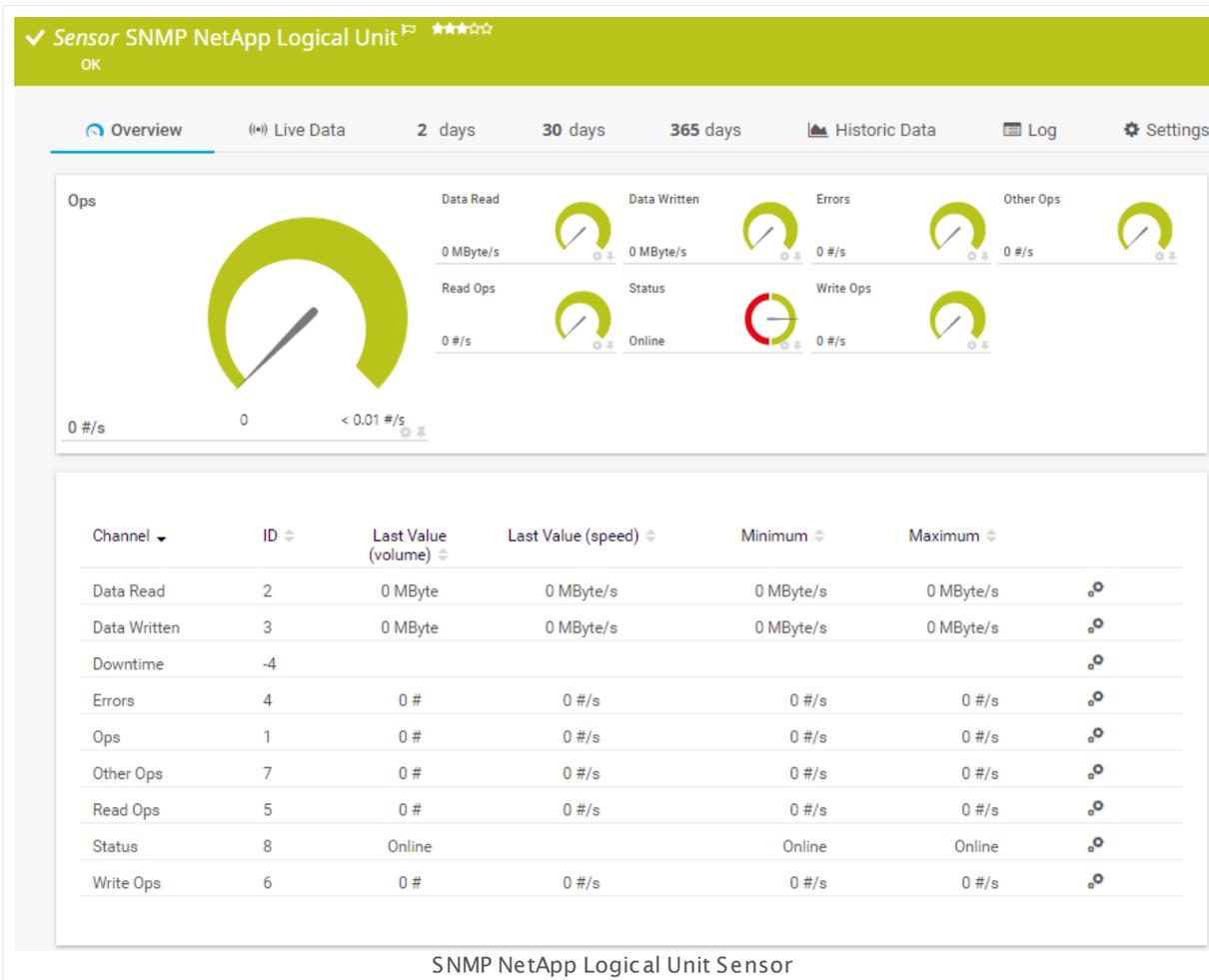
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.177 SNMP NetApp Logical Unit Sensor

The SNMP NetApp Logical Unit sensor monitors the input/output operations (IOPS) on a logical unit of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Total number of operations per second
- Data read speed
- Data write speed
- Number of errors per second
- Number of read operations per second
- Number of write operations per second
- Number of other operations per second
- Status of the logical unit (online or offline)



Sensor in Other Languages

Dutch: **SNMP NetApp Logical Unit**, French: **Unité logique NetApp SNMP**, German: **SNMP NetApp Logische Unit**, Japanese: **SNMP NetApp ? ? ? ? ? ?**, Portuguese: **Unidade lógica SNMP NetApp**, Russian: **Логический блок NetApp по SNMP**, Simplified Chinese: **SNMP NetApp ? ? ? ?**, Spanish: **Unidad lógica NetApp por SNMP**

Remarks

- This sensor type only supports NetApp versions up to 8.2.
- If you use NetApp cDOT 8.3 or NetApp ONTAP 9.0 or later, we recommend that you use the [NetApp LUN sensor](#)¹³³⁴ instead.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical units on the NetApp you want to monitor. PRTG creates one sensor for each unit you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP DISK FREE SETTINGS

Logical Unit	Select the logical units you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP LOGICAL UNIT SETTINGS

Logical Unit	Shows the name of the logical unit that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
--------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

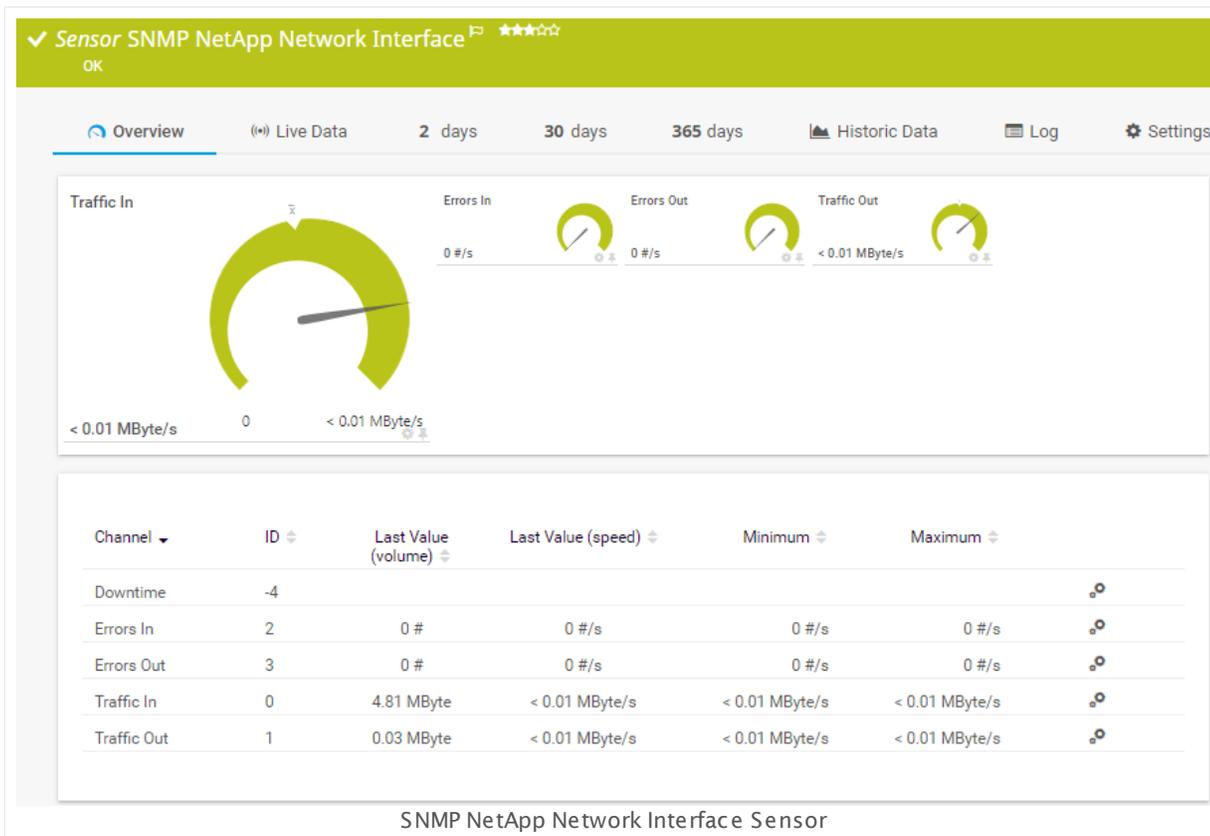
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.178 SNMP NetApp Network Interface Sensor

The SNMP NetApp Network Interface sensor monitors a network card of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- Traffic in
- Traffic out
- Number of errors per second (in and out).



Sensor in Other Languages

Dutch: **SNMP NetApp Network Interface**, French: **Interface réseau NetApp SNMP**, German: **SNMP NetApp Netzwerkschnittstelle**, Japanese: **SNMP NetApp** ? ? ? ? ? ? ? ? ? ? ? ? ? ? , Portuguese: **Interface de rede SNMP NetApp**, Russian: **Сетевой интерфейс NetApp по SNMP**, Simplified Chinese: **SNMP NetApp** ? ? ? ? , Spanish: **SNMP Interface de red NetApp**

Remarks

- This sensor type only supports NetApp versions up to 8.2.
- If you use NetApp cDOT 8.3 or NetApp ONTAP 9.0 or later, we recommend that you use the [NetApp NIC sensor](#) ¹³⁴⁵ instead.

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network interfaces on the NetApp you want to monitor. PRTG will create one sensor for each interface you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

NETAPP NETWORK INTERFACE SETTINGS

Network Interface Select the interfaces you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3270], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

NETAPP NETWORK INTERFACE SETTINGS

- Network Interface** Shows the name of the interface that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

i This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

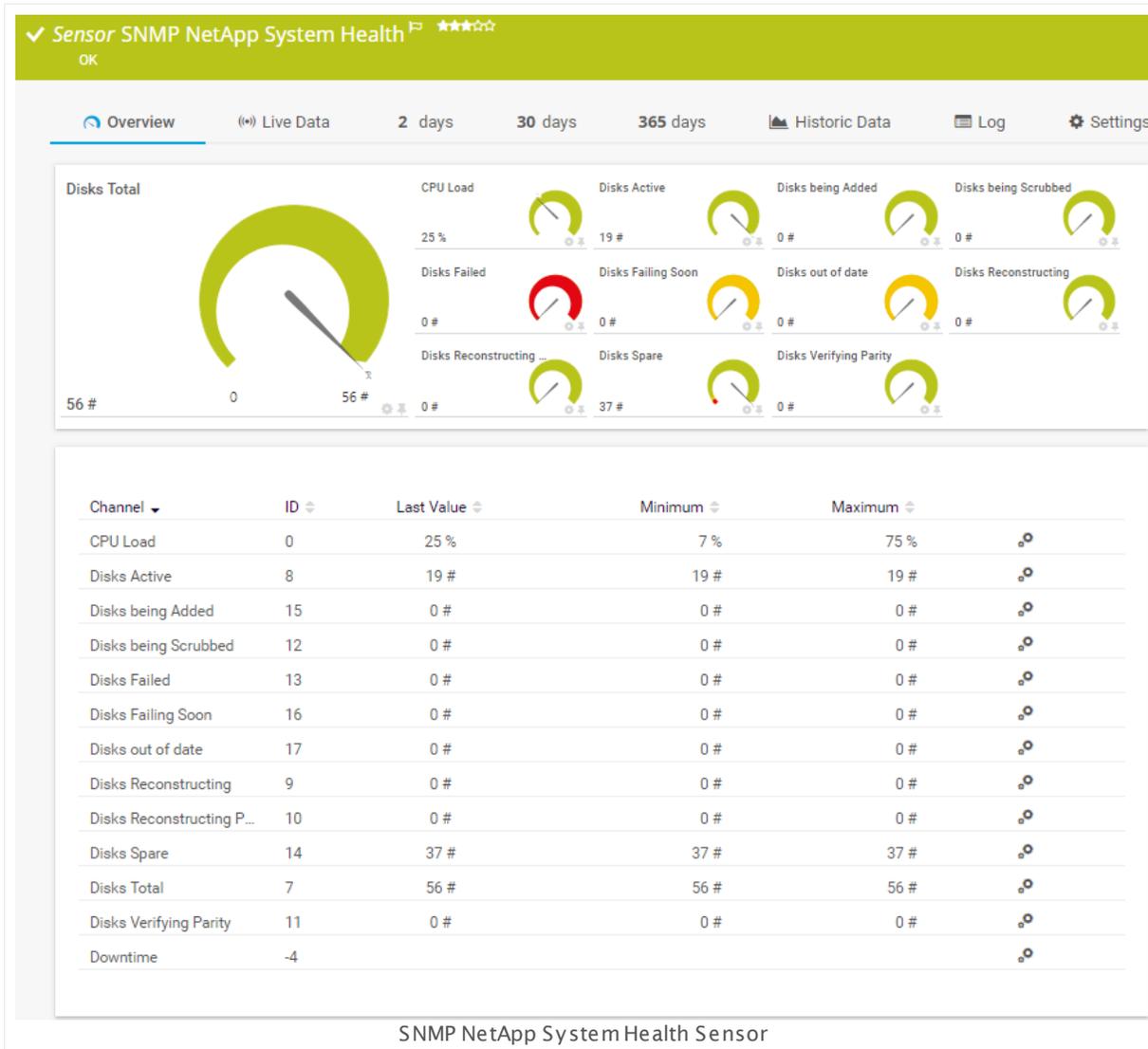
7.8.179 SNMP NetApp System Health Sensor

The SNMP NetApp System Health sensor monitors the status of a NetApp storage system via Simple Network Management Protocol (SNMP).

It can show the following:

- CPU load in percent
- Number of active restores
- Number of current CIFS users
- Number of active disks
- Number of disks being added
- Number of disks being scrubbed
- Number of failed disks
- Number of soon failing disks
- Number of disks being out of date
- Number of reconstructing (parity) disks
- Number of spare disks
- Total number of disks
- Number of verifying (parity) disks
- Number of failed fans
- Number of failed power supplies
- Maximum used disk space in percent
- Maximum used INodes in percent
- If the environment is over temperature

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP NetApp Systeemstatus**, French: **Intégrité du système Net App SNMP**, German: **SNMP NetApp Systemzustand**, Japanese: **SNMP NetApp ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema SNMP NetApp**, Russian: **Работоспособность системы NetApp по SNMP**, Simplified Chinese: **SNMP NetApp ? ? ? ? ? ? ?**, Spanish: **SNMP Salud de sistema NetApp**

Remarks

- If you use NetApp cDOT 8.3 or NetApp ONTAP 9.0 or later, we recommend that you use the [NetApp System Health sensor](#)¹³⁷⁹ instead.
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)³⁴⁸⁹.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

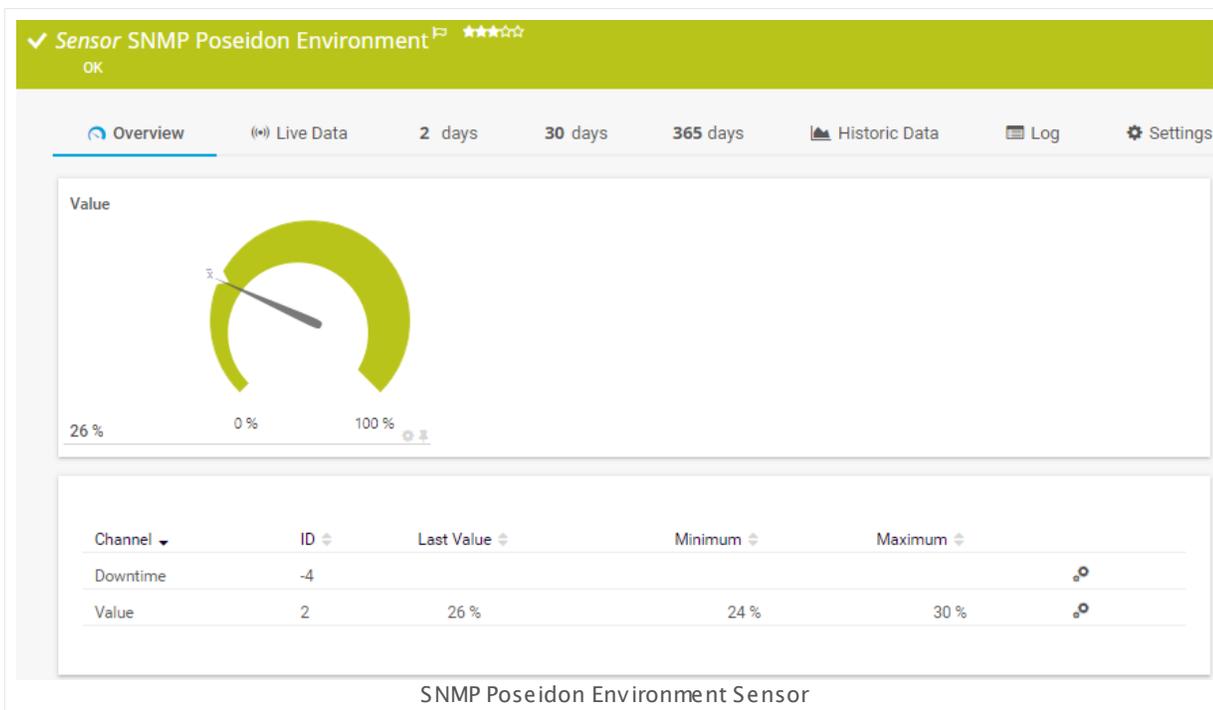
7.8.180 SNMP Poseidon Environment Sensor

The SNMP Poseidon Environment sensor monitors performance counters for environmental measurements on Poseidon hardware via Simple Network Management Protocol (SNMP).

It can show, depending on available measurement components on the hardware device and what measurement you choose:

- Humidity
- Temperature

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP Poseidon Omgeving**, French: **Environnement Poseidon SNMP**, German: **SNMP Poseidon-Umgebung**, Japanese: **SNMP Poseidon ? ? ? ?**, Portuguese: **Ambiente Poseidon SNMP**, Russian: **Окружающая среда Poseidon по SNMP**, Simplified Chinese: **SNMP Poseidon ? ?**, Spanish: **Entorno Poseidon con SNMP**

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) 3489.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

To monitor performance counters for environmental measurements on Poseidon hardware, PRTG will create one sensor for each measuring point you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

POSEIDON ENVIRONMENT SPECIFIC

Measuring Point Select the measurements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

POSEIDON ENVIRONMENT SPECIFIC

Name	Shows further information about the measurement. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Unit	
Measuring Point	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

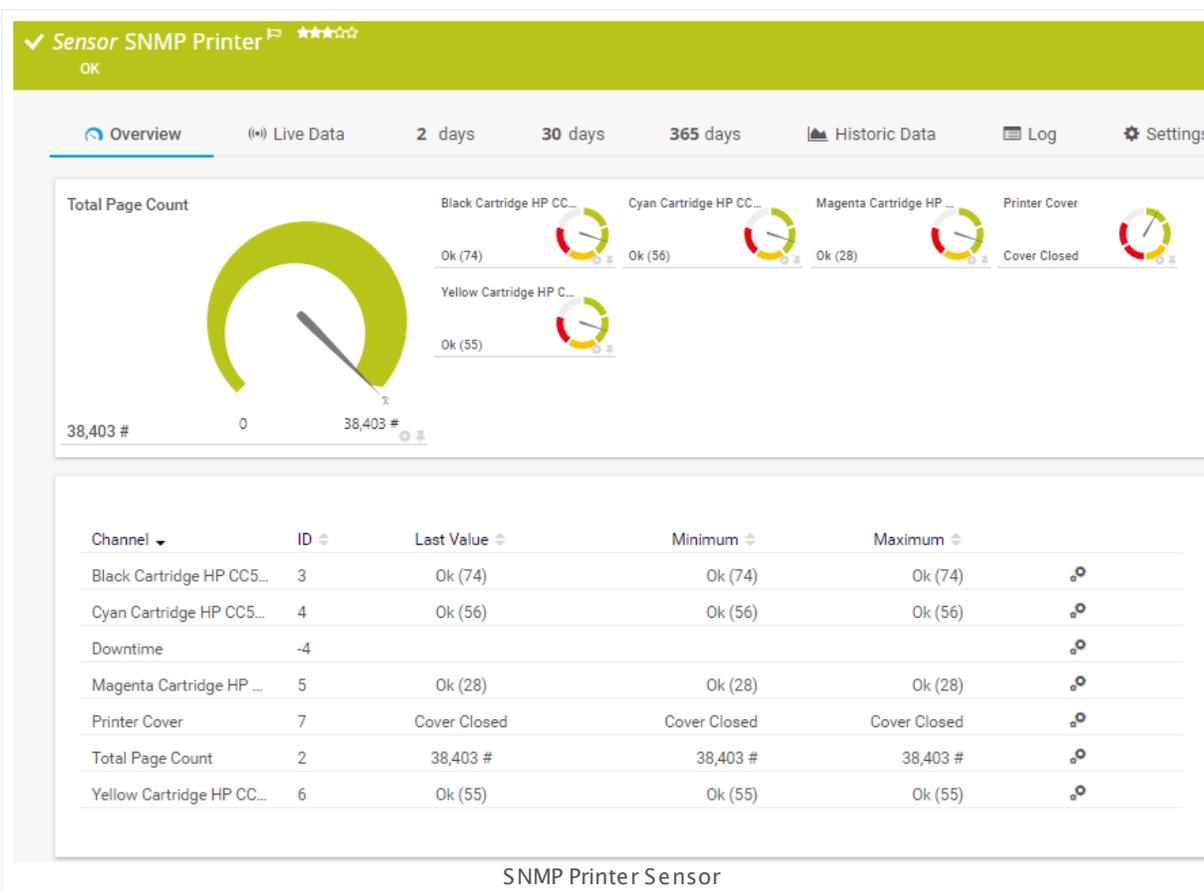
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.181 SNMP Printer Sensor

The SNMP Printer sensor is a generic sensor that monitors various types of printers via Simple Network Management Protocol (SNMP).

It can show the following:

- Total number of printed pages
- Fill level of cartridges and toners
- Status of the printer cover
- Additionally, the sensor shows the printer status as sensor message.



Sensor in Other Languages

Dutch: **SNMP Printer**, French: **Imprimante SNMP**, German: **SNMP-Drucker**, Japanese: **SNMP ? ? ? ?**, Portuguese: **Impressora de SNMP**, Russian: **Принтер по SNMP**, Simplified Chinese: **SNMP ? ? ?**, Spanish: **Impresora de SNMP**

Remarks

- This sensor type supports the following printers, among others: HP OfficeJet printers, HP LaserJet printers, RICOH SP 5200, SP 3410, SP C242DN, MP C3003, MP C2503

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.
- If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
-  Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
-  If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
-  If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

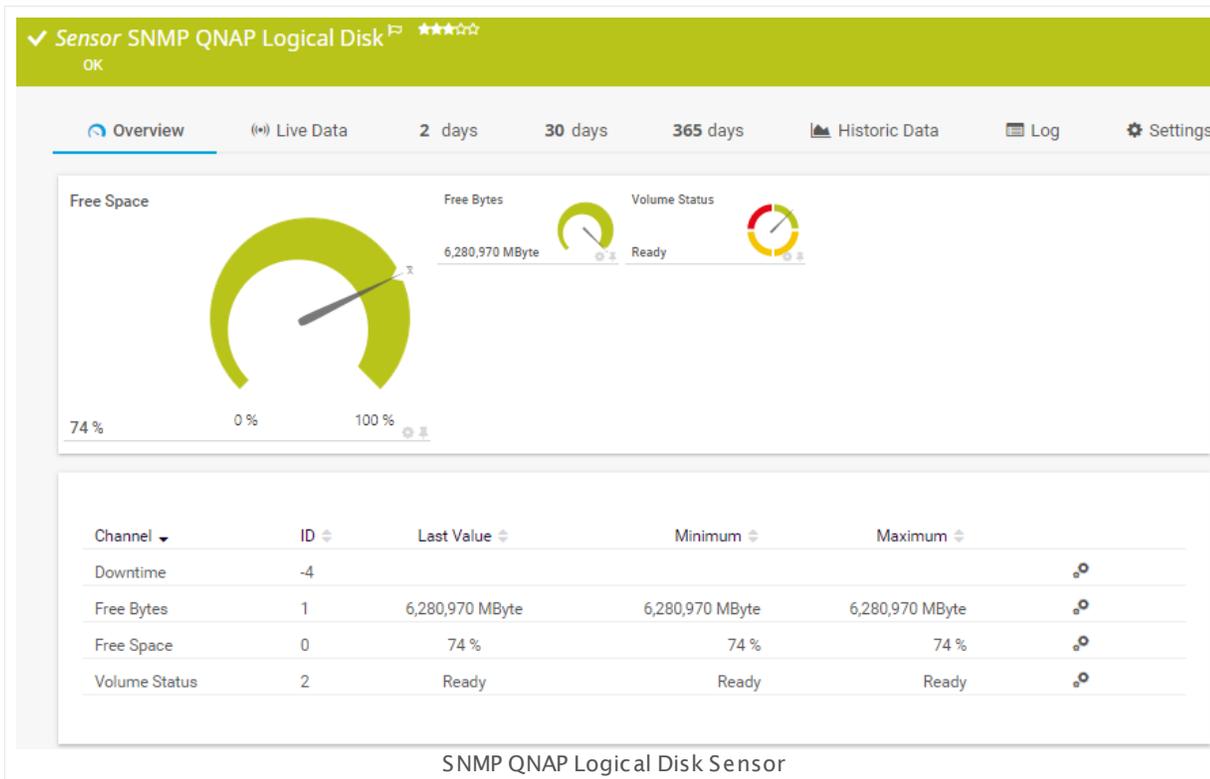
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.182 SNMP QNAP Logical Disk Sensor

The SNMP QNAP Logical Disk sensor monitors a logical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Free disk space in percent
- Free disk space in bytes
- Status of the volume
 - **Up status** ¹⁹⁵: ready
 - **Warning** status: rebuilding, in degraded mode, synchronizing
 - **Down** status: failure



Sensor in Other Languages

Dutch: **SNMP QNAP Logische Schijf**, French: **Disque logique QNAP SNMP**, German: **SNMP QNAP Logischer Datenträger**, Japanese: **SNMP QNAP ? ? ? ? ?**, Portuguese: **Disco lógico QNAP SNMP**, Russian: **Логический диск QNAP по SNMP**, Simplified Chinese: **SNMP QNAP ? ? ?**, Spanish: **Disco lógico de QNAP con SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks in the QNAP NAS you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Disk	Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Disk	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value.
Description	It is shown for reference purposes only. If you need to change this, please add the sensor anew.
File System	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why do I get DoS Alarms on my QNAP?

- <https://kb.paessler.com/en/topic/80421>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
182 SNMP QNAP Logical Disk Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

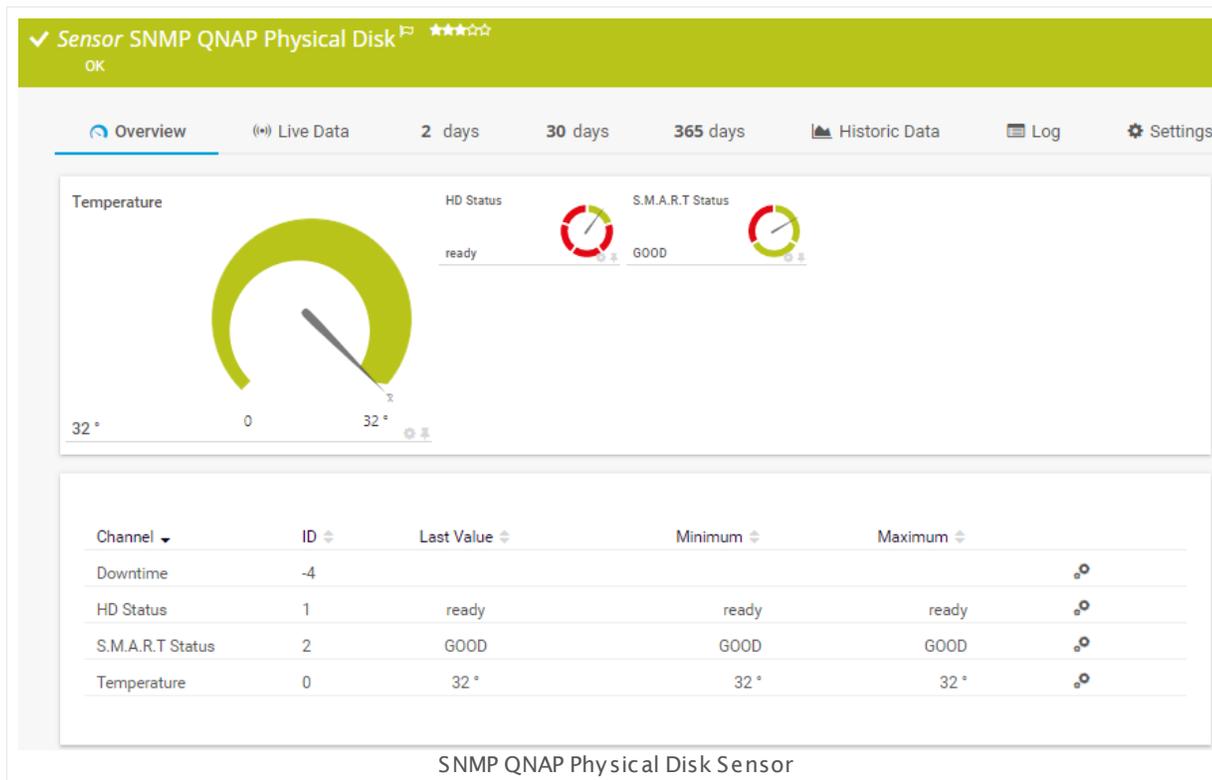
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.183 SNMP QNAP Physical Disk Sensor

The SNMP QNAP Physical Disk sensor monitors a physical disk in a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Temperature
- Disk status
- Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) status of the disk.



Sensor in Other Languages

Dutch: **SNMP QNAP Fysieke Schijf**, French: **Disque physique QNAP SNMP**, German: **SNMP QNAP Physikalischer Datenträger**, Japanese: **SNMP QNAP ? ? ? ? ? ?**, Portuguese: **Disco físico QNAP SNMP**, Russian: **Физический диск QNAP по SNMP**, Simplified Chinese: **SNMP QNAP ? ? ? ?**, Spanish: **Disco físico de QNAP con SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#) [3693].

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the QNAP NAS you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. You can also define the unit of the temperature measurement. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Disk	Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
Unit	Select the unit of the temperature measurement. Choose between Celsius and Fahrenheit .

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Disk	Shows further information about the disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Description	
Model	
Capacity	
Unit	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why do I get DoS Alarms on my QNAP?

- <https://kb.paessler.com/en/topic/80421>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

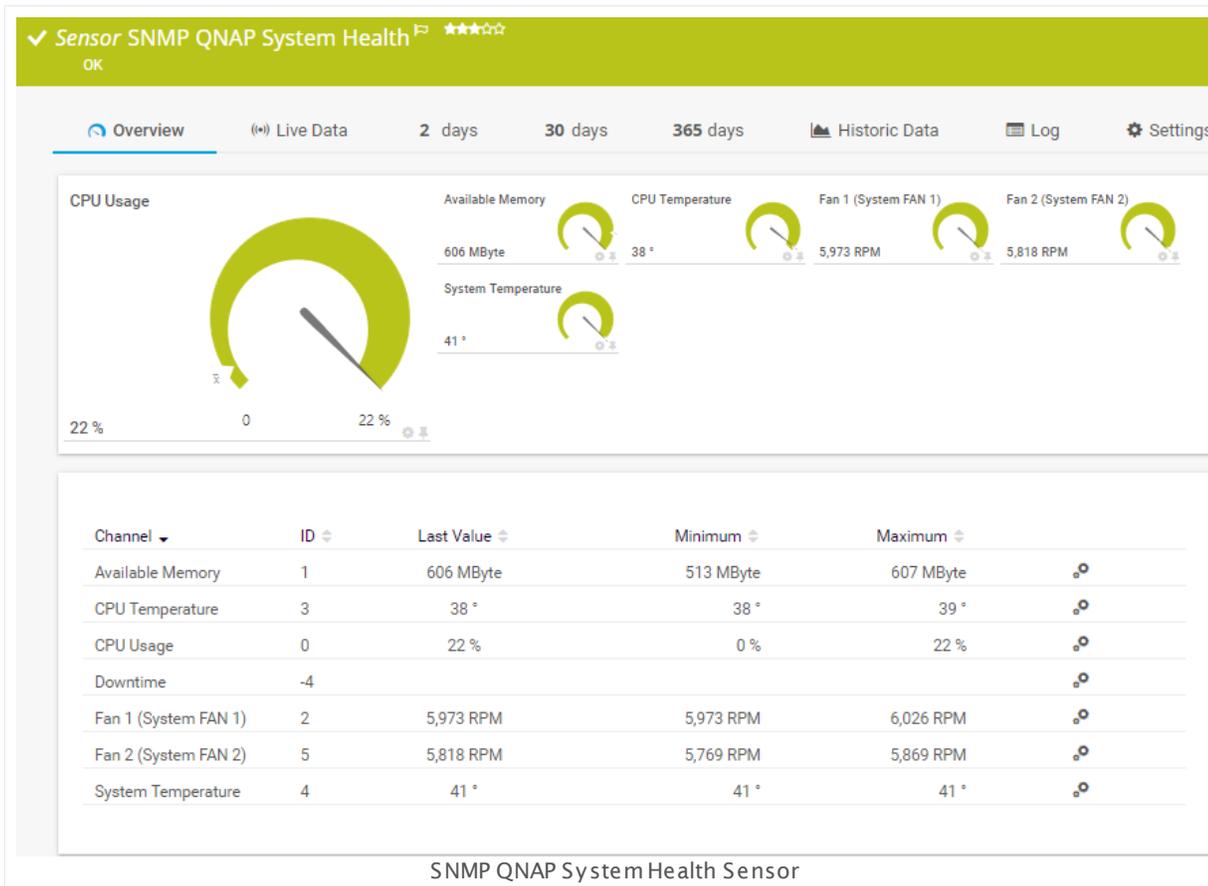
7.8.184 SNMP QNAP System Health Sensor

The SNMP QNAP System Health sensor monitors the system health of a QNAP Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following, depending on the available measurement components:

- CPU usage in percent
- Available memory in bytes
- Temperature of CPU
- Temperature of system
- Revolutions of fans per minute (RPM)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SNMP QNAP Systeemstatus**, French: **État du système QNAP SNMP**, German: **SNMP QNAP Systemzustand**, Japanese: **SNMP QNAP ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema QNAP SNMP**, Russian: **Работоспособность системы QNAP по SNMP**, Simplified Chinese:

SNMP QNAP ? ? ? ? ? , Spanish: **Salud del sistema de QNAP con SNMP**

Remarks

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

To monitor the system health of a QNAP NAS, specify the unit of the temperature measurement.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

QNAP NAS SETTINGS

Unit Select the unit of the temperature measurement. Choose between **Celsius** and **Fahrenheit**.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3276], [libraries](#)^[3235], and [tickets](#)^[230].

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

QNAP NAS SETTINGS

Unit	Shows the unit of temperatures as monitored with this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why do I get DoS Alarms on my QNAP?

- <https://kb.paessler.com/en/topic/80421>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
184 SNMP QNAP System Health Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.185 SNMP RMON Sensor

The SNMP RMON sensor monitors traffic on a device using the Remote Monitoring (RMON) standard via Simple Network Management Protocol (SNMP). You can create it on an SNMP compatible device that provides traffic data via RMON. Depending on the data returned by your device, traffic data for each port can be displayed in different channels, allowing detailed analysis. If available, the sensor queries 64-bit counters.

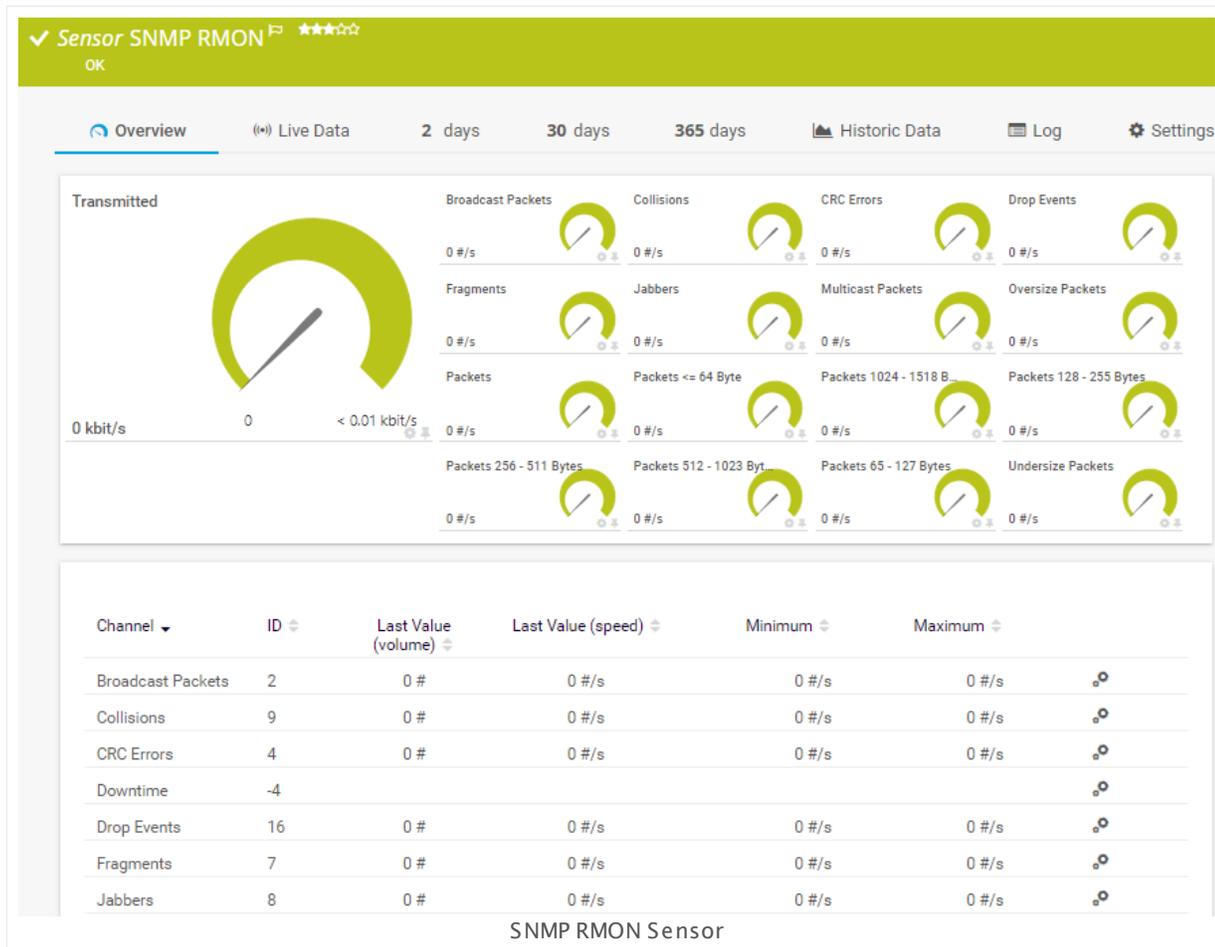
For each port, the sensor can show, for example:

- Transmitted kbit/s
- Packets (#/s)
- Broadcast Packets (#/s)
- Multicast Packets (#/s)
- CRC Errors (#/s)
- Undersize Packets (#/s)
- Oversize Packets (#/s)
- Fragments (#/s)
- Jabbers (#/s)
- Collisions (#/s)
- Packets <= 64 Byte (#/s)
- Packets 65 - 127 Bytes (#/s)
- Packets 128 - 255 Bytes (#/s)
- Packets 256 - 511 Bytes (#/s)
- Packets 512 - 1023 Bytes (#/s)
- Packets 1024 - 1518 Bytes (#/s)
- Drop Events (#/s)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

185 SNMP RMON Sensor



Remarks

- You can define the displayed sensor name with port name templates in the [SNMP Compatibility Options](#)^[416] of the parent device.
- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#)^[317] with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [What value does the "Transmitted" channel of an RMON sensor show?](#)
- Knowledge Base: [How do PRTG's automatic port name and number updates work for SNMP traffic sensors?](#)
- Knowledge Base: [Where is the volume line in graphs?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ports you want to monitor. PRTG will create one sensor for each port you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

RMON SPECIFIC

Ports Select the ports you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

RMON SPECIFIC

Port	<p>Shows the number of the interface port in your physical device that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Channel Mask	<p>Describes which channels are available and might be useful for technical support. This setting is shown for your information only and cannot be changed here.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.</p>
Chart Type	<p>Define how to show different channels for this sensor.</p>

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.
- **Show in and out traffic as positive and negative area chart:** Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way.
 - ⓘ You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.
 - ⓘ You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the [Sensor Channels Settings](#)³¹⁶⁰).

Stack Unit

This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

SCANNING INTERVAL

- Scanning Interval** Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#) on PRTG on premises installations.
- If a Sensor Query Fails** Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:
- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: What value does the "Transmitted" channel of an RMON sensor show?

- <https://kb.paessler.com/en/topic/59821>

Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

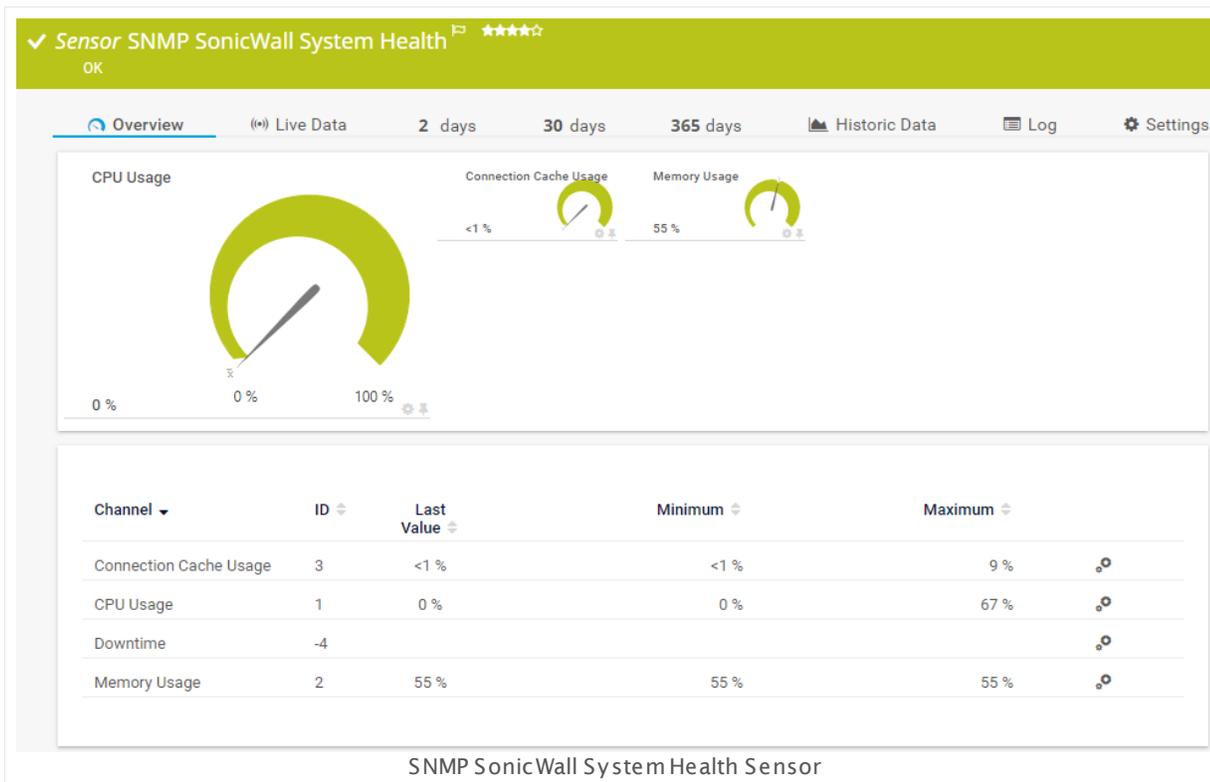
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.186 SNMP SonicWall System Health Sensor

The SNMP SonicWall System Health sensor monitors health values of a Dell SonicWall Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP).

It shows the following:

- CPU usage in percent
- Memory usage in percent
- Connection cache usage in percent



Sensor in Other Languages

Dutch: **SNMP SonicWall System Health**, French: **État du système SNMP SonicWall**, German: **SNMP SonicWall Systemzustand**, Japanese: **SNMP SonicWall** ? ? ? ? ? ? ? , Portuguese: **Funcionamento do sistema SonicWall SNMP**, Russian: **Работоспособность системы SonicWall по SNMP**, Simplified Chinese: **SNMP SonicWall** ? ? ? ? ? ? ? , Spanish: **Salud del sistema de SonicWall de SNMP**

Remarks

- Knowledge Base: [Why does PRTG write error messages into my SonicWALL log?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) [3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why does PRTG write error messages into my SonicWALL log?

- <https://kb.paessler.com/en/topic/61961>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

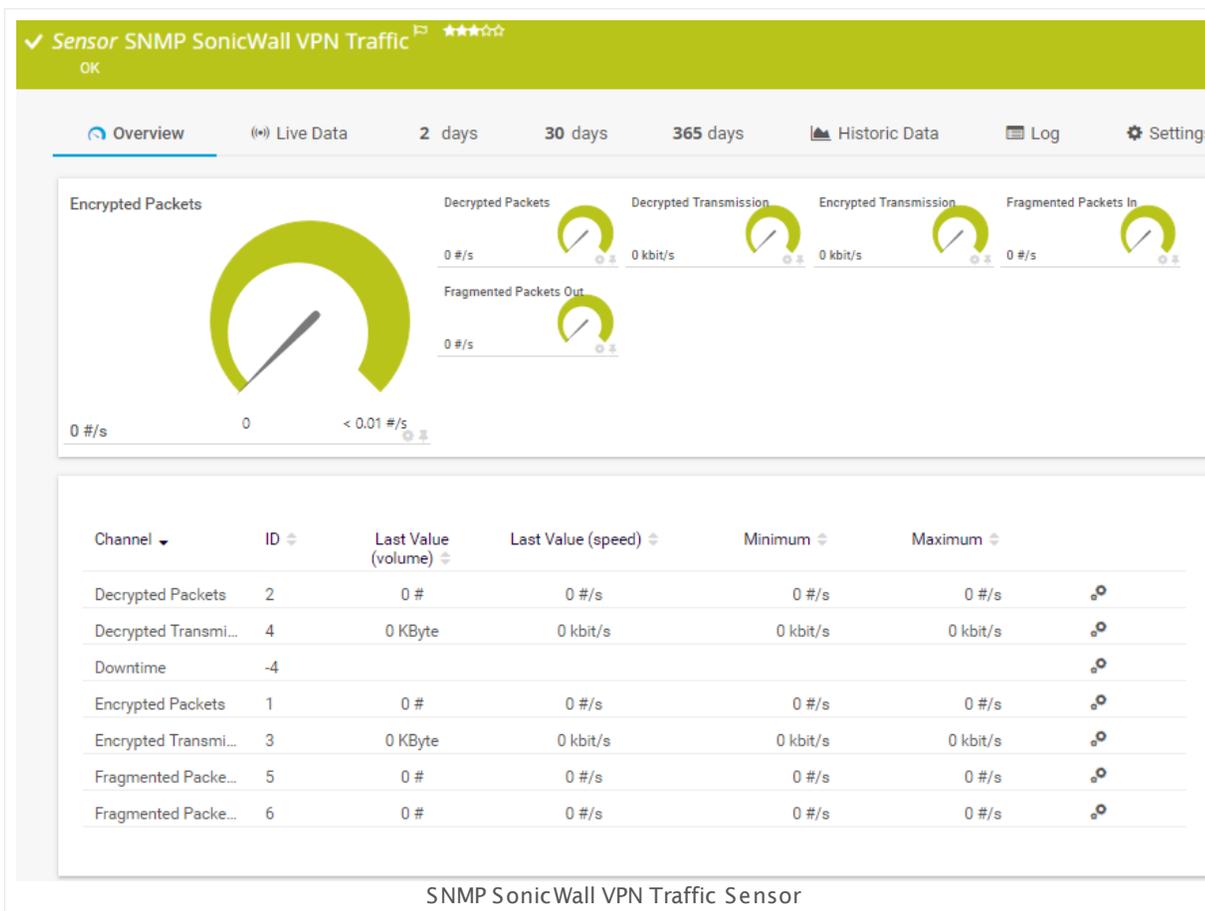
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.187 SNMP SonicWall VPN Traffic Sensor

The SNMP SonicWall VPN Traffic sensor monitors the traffic of an Internet Protocol Security (IPsec) Virtual Private Network (VPN) on a Dell SonicWall Network Security Appliance (NSA) via Simple Network Management Protocol (SNMP).

It can show the following:

- Number of encrypted and decrypted packets per second
- Bytes of encrypted and decrypted transmissions per second
- Number of ingoing and outgoing fragmented packets per second



Sensor in Other Languages

Dutch: **SNMP SonicWall VPN Verkeer**, French: **Traffic VPN SonicWall SNMP**, German: **SNMP SonicWall VPN-Datenverkehr**, Japanese: **SNMP SonicWall VPN** , Portuguese: **Tráfego VPN SonicWall via SNMP**, Russian: **Трафик VPN SonicWall по SNMP**, Simplified Chinese: **SNMP SonicWall VPN** , Spanish: **Tráfico SNMP de VPN SonicWall**

Remarks

- Knowledge Base: [Why does PRTG write error messages into my SonicWALL log?](#)

- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the connections of the SonicWall VPN you want to monitor. PRTG will create one sensor for each connection you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SONICWALL VPN SPECIFIC

Connections	Select the connections you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
Identification Method	Define how you want to identify the connection that you want to monitor. PRTG always uses the first connection found that matches all criteria. Choose between: <ul style="list-style-type: none">▪ By index: Every connection has a unique index. This is the safest method to identify your connection. Though, if the connection is lost and reconnected, a new index will be assigned.▪ By remote IP: If the target of the VPN always has the same IP, you can use this IP to identify the connection.▪ By security policy name: If you use a different security policy for every VPN, you can use its name to identify the connection.▪ By remote IP and security policy name: You can also combine both identification methods.▪ By remote IP, security policy name, and IP ranges: If you use separate connections for specific IP ranges, identify the connection by remote IP, security policy name, and IP ranges.▪ By IP ranges: Use IP ranges only to identify the connection.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SONICWALL VPN SPECIFIC

Security Policy	Shows information about the monitored connection. Once a sensor is created, you cannot change this value. It is shown for reference purposes only.
Remote IP	If you need to change this, please add the sensor anew.
Source IPs	

SONICWALL VPN SPECIFIC

Destination IPs

Index

Identification Method

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>[3311]</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: Why does PRTG write error messages into my SonicWALL log?

- <https://kb.paessler.com/en/topic/61961>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

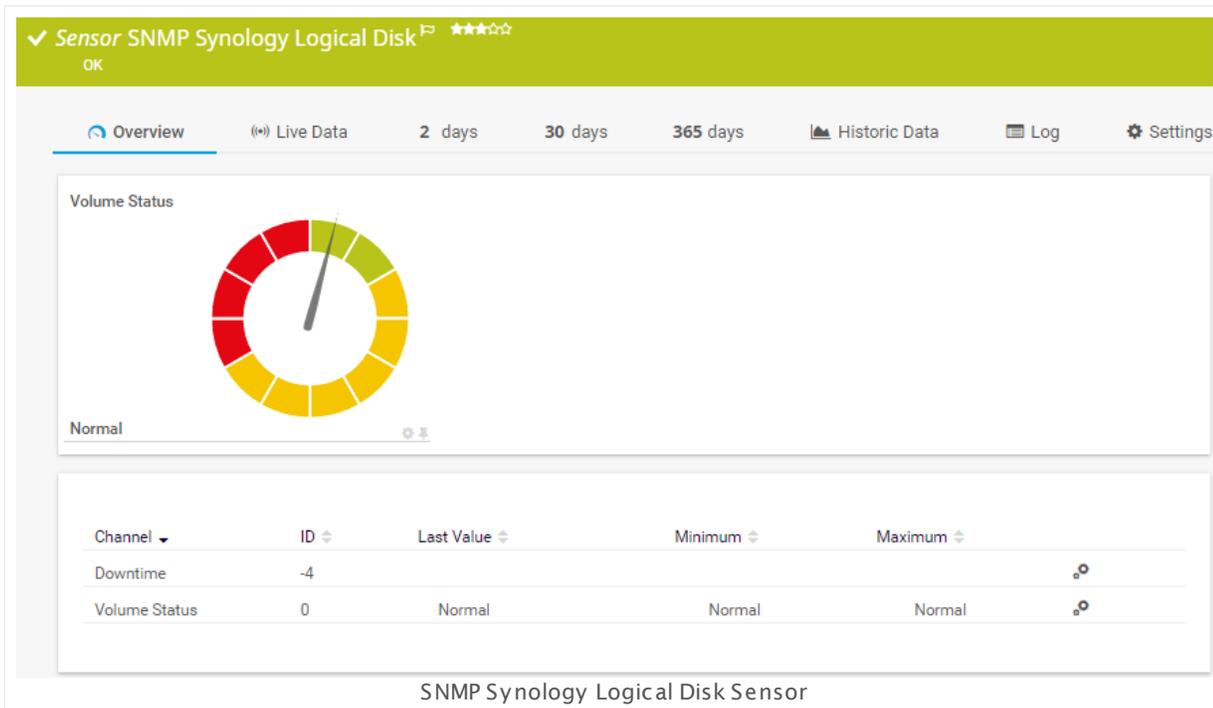
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.188 SNMP Synology Logical Disk Sensor

The SNMP Synology Logical Disk sensor monitors a logical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

- It can show the status of a volume.



Sensor in Other Languages

Dutch: **SNMP Synology Logische Schijf**, French: **Disque logique Synology SNMP**, German: **SNMP Synology Logischer Datenträger**, Japanese: **SNMP Synology** , Portuguese: **Disco lógico Synology SNMP**, Russian: **Логический диск Synology по SNMP**, Simplified Chinese: **SNMP Synology** , Spanish: **Disco lógico de Synology con SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks in the Synology NAS that you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SYNOLOGY NAS SETTINGS

Disk Select the logical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) [402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#) [181], as well as in [alarms](#) [219], [logs](#) [228], [notifications](#) [3216], [reports](#) [3252], [maps](#) [3276], [libraries](#) [3235], and [tickets](#) [230].

Parent Tags Shows [Tags](#) [139] that this sensor [inherits](#) [140] from its [parent device, group, and probe](#) [133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#) [139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) [140] from objects further up in the device tree. These are visible above as **Parent Tags**.

BASIC SENSOR SETTINGS

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SYNOLOGY NAS SETTINGS

Disk Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

i This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

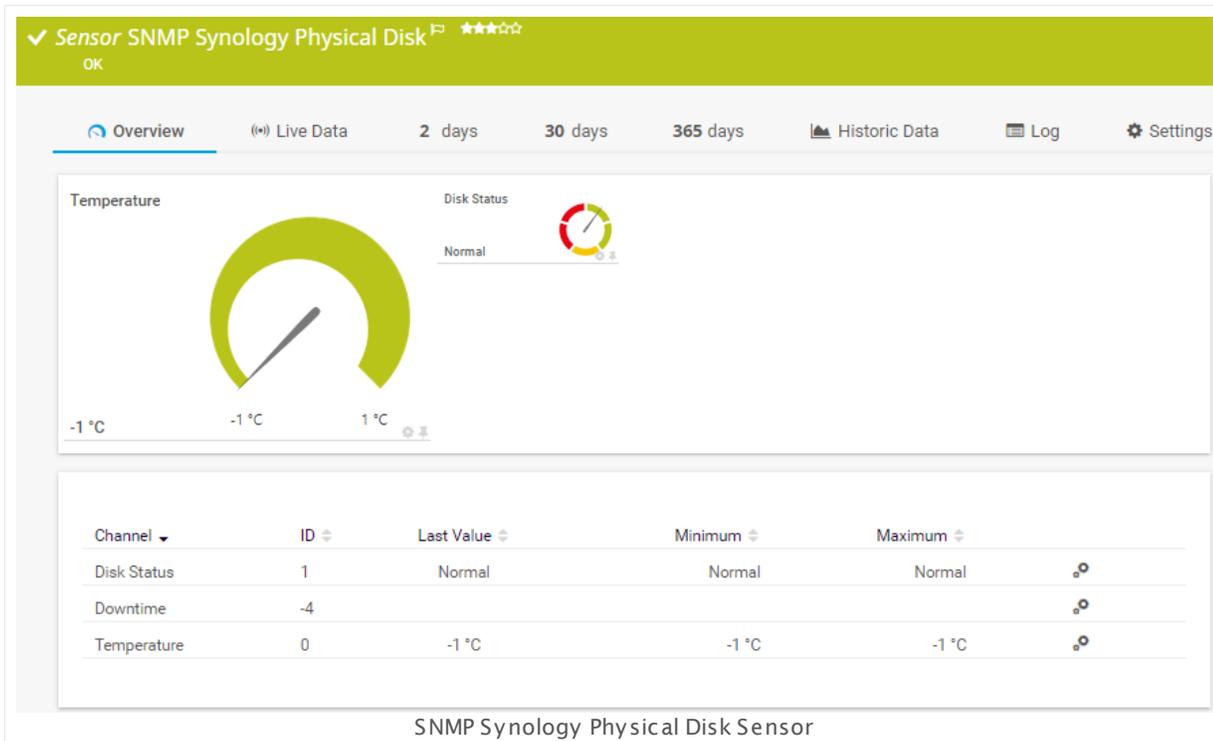
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.189 SNMP Synology Physical Disk Sensor

The SNMP Synology Physical Disk sensor monitors a physical disk in a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following:

- Temperature
- Disk status



Sensor in Other Languages

Dutch: **SNMP-Synology Fysieke Schijf**, French: **Disque physique Synology SNMP**, German: **SNMP Synology Physikalischer Datenträger**, Japanese: **SNMP Synology ? ? ? ? ? ?**, Portuguese: **Disco físico Synology SNMP**, Russian: **Физический диск Synology по SNMP**, Simplified Chinese: **SNMP Synology ? ? ? ?**, Spanish: **Disco físico de Synology con SNMP**

Remarks

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disks in the Synology NAS you want to monitor. PRTG will create one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SYNOLOGY NAS SETTINGS

Disk Select the physical disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SYNOLOGY NAS SETTINGS

Disk	Shows further information about the disk that this sensor monitors. Once a sensor is created, you cannot change this value.
Name	It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Model	
Type	

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
189 SNMP Synology Physical Disk Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.190 SNMP Synology System Health Sensor

The SNMP Synology System Health sensor monitors the system health of a Synology Network Attached Storage (NAS) via Simple Network Management Protocol (SNMP).

It can show the following, depending on the available measurement components:

- Temperature (if available on the target device)
- System status
- Power status
- Fan status
- Memory usage in percent
- CPU load in percent

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

 For more information about the shown memory and CPU load values, see the Knowledge Base: [Why does my Synology System Health sensor show incorrect CPU and memory values?](#)

✓ Sensor SNMP Synology System Health ★★★★☆

OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

System Status



Normal

CPU Fan Status



Normal

CPU Load



0 %

Memory Free



81 %

Temperature



40 °C

Channel	ID	Last Value	Minimum	Maximum	
CPU Fan Status	4	Normal	Normal	Normal	
CPU Load	3	0 %	0 %	64 %	
Downtime	-4				
Memory Free	2	81 %	81 %	82 %	
System Status	1	Normal	Normal	Normal	
Temperature	0	40 °C	40 °C	40 °C	

SNMP Synology System Health Sensor

Sensor in Other Languages

Dutch: **SNMP-Synology Systeem Status**, French: **État du système Synology SNMP**, German: **SNMP Synology Systemzustand**, Japanese: **SNMP Synology ? ? ? ? ? ? ?**, Portuguese: **Funcionamento do sistema Synology SNMP**, Russian: **Работоспособность системы Synology no SNMP**, Simplified Chinese: **SNMP Synology ? ? ? ? ?**, Spanish: **Salud del sistema de Synology con SNMP**

Remarks

- Knowledge Base: [Why does my Synology System Health sensor show incorrect CPU and memory values?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
- i** It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- i** You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
- i** This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)^[3160] settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Why does my Synology System Health sensor show incorrect CPU and memory values?

- <https://kb.paessler.com/en/topic/63283>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

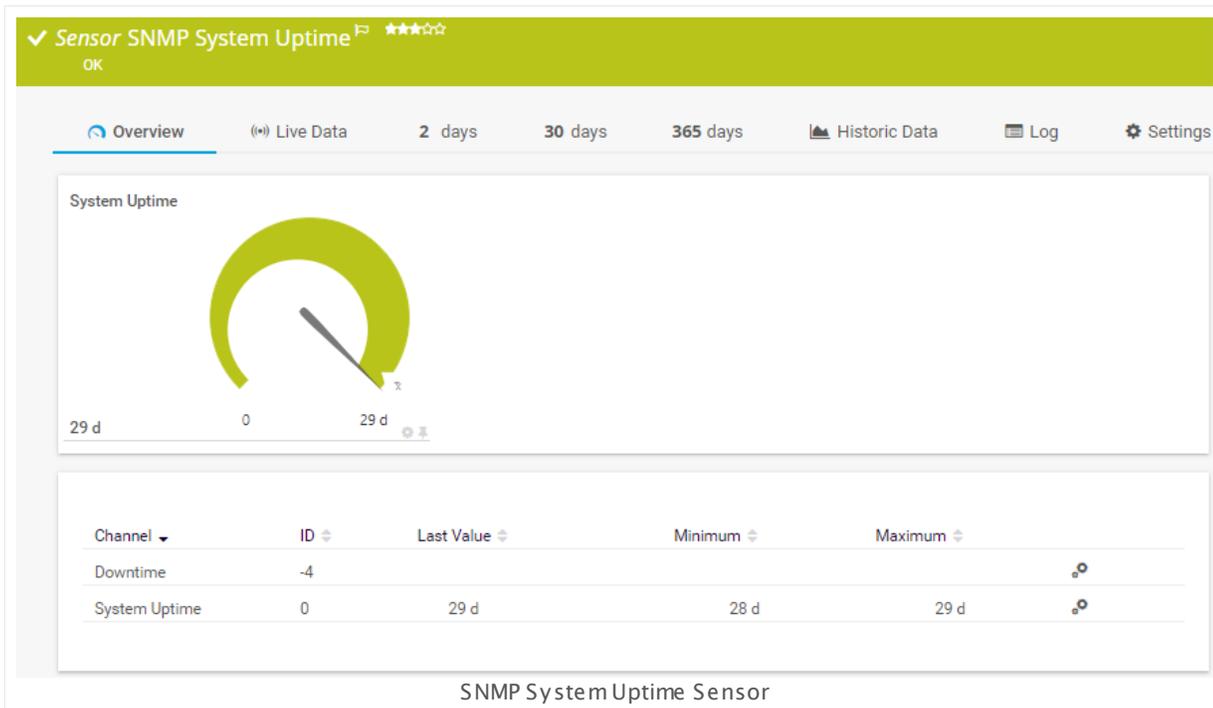
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.191 SNMP System Uptime Sensor

The SNMP System Uptime sensor monitors the time a device is running via Simple Network Management Protocol (SNMP).

- It reads the system uptime value of the monitored device and shows it.



Sensor in Other Languages

Dutch: **SNMP System Uptime**, French: **Disponibilité du système SNMP**, German: **SNMP-Laufzeit**, Japanese: **SNMP ? ? ? ? ? ? ? ?**, Portuguese: **Tempo de atividade do sistema SNMP**, Russian: **Время бесперебойной работы системы по SNMP**, Simplified Chinese: **SNMP ? ? ? ? ? ? ? ?**, Spanish: **Disponibilidad SNMP**

Remarks

- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [Why does the SNMP System Uptime sensor report wrong values?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Why does the SNMP System Uptime sensor report wrong values?

- <https://kb.paessler.com/en/topic/61249>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
191 SNMP System Uptime Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.192 SNMP Traffic Sensor

The SNMP Traffic sensor monitors traffic on a device using Simple Network Management Protocol (SNMP). You can create it on a device that provides traffic data, one traffic sensor for each individual port.

It can show the following:

- Traffic in
- Traffic out
- Traffic total

You can also add additional channels:

- Errors in and out
- Discards in and out
- Unicast packets in and out
- Non unicast packets in and out
- Multicast packets in and out
- Broadcast packets in and out
- Unknown protocols

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

192 SNMP Traffic Sensor



Sensor in Other Languages

Dutch: **SNMP Verkeer**, French: **Traffic SNMP**, German: **SNMP-Datenverkehr**, Japanese: **SNMP ? ? ? ? ?**, Portuguese: **Tráfego SNMP**, Russian: **Трафик по SNMP**, Simplified Chinese: **SNMP ? ?**, Spanish: **SNMP tráfico**

Remarks

- You can define the displayed sensor name with port name templates in the [SNMP Compatibility Options](#) of the parent device.
- We recommend that you choose SNMP v2c (most common) or SNMP v3 in the [Credentials for SNMP Devices](#) of the parent device (if supported by the device that you monitor). SNMP v1 does not support 64-bit counters, which may result in invalid data. For details, see the Knowledge Base: [Querying 64-bit Counters with SNMP Traffic Sensors](#)
- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#) with the IP address that it has in your network and create the SNMP sensor on this device instead.
- Knowledge Base: [How do PRTG's automatic port name and number updates work for SNMP traffic sensors?](#)
- Knowledge Base: [Where is the volume line in graphs?](#)
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ports on SNMP devices with multiple interfaces you want to monitor. PRTG will create one sensor for each port you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

TRAFFIC SPECIFIC

Interface Number You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 You can see the connection status of an interface in the respective table column.

 You can group-select and deselect interfaces by using the buttons **Select all connected interfaces**, **Select all disconnected interfaces**, and **Deselect all interfaces**.

Description "IN" Channel For the standard channel **Traffic In**, enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor [channel settings](#)³¹⁶⁰ later.

Description "OUT" Channel For the standard channel **Traffic Out**, enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor [channel settings](#)³¹⁶⁰ later.

Description "TOTAL" Channel For the standard channel **Traffic Total**, enter the channel name here. The sensor shows it in graphs and tables. You can change this description and the description of all other channels in the sensor [channel settings](#)³¹⁶⁰ later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

TRAFFIC SPECIFIC

Interface Number Shows the number and name of the interface in your physical device that this sensor monitors. This value is shown for reference purposes only. We strongly recommend that you only change it if Paessler support explicitly asks you to do so. Wrong usage can result in incorrect monitoring data!

Additional Channels By default, each SNMP Traffic sensor will create the channels **Traffic In**, **Traffic Out**, and **Traffic Total**. Choose additional channels for all selected interfaces. Click on the respective channel name(s) to mark them and monitor their data.

You can choose from the following additional channels:

- **Errors In & Out**: The number of in-/outbound packets that could not be delivered because of errors.
- **Discards In & Out**: The number of discarded in-/outbound packets even though no errors had been detected.
- **Unicast Packets In & Out**: The number of unicast packets that were delivered.
- **Non Unicast Packets In & Out (32-bit only)**: The number of non-unicast packets that were delivered.
- **Multicast Packets In & Out (64-bit only)**: The number of delivered packets that were addressed to a multicast address.
- **Broadcast Packets In & Out (64-bit only)**: The number of delivered packets that were addressed to a broadcast address.
- **Unknown Protocols**: The number of received packets that were discarded because of an unknown or unsupported protocol.

 Channels that are once created cannot be deleted later. You can disable them only.

Connection Status Handling Define how PRTG will react when an interface is operational. An interface that is not operational is, for example, an ethernet port on a switch with no cable plugged in. This setting is valid for all interfaces selected above. Choose between:

- **Show alarm for all "disconnected" states**: The sensor for the interface will always turn into a red **Down status**^[195] for a disconnected interface. This applies if the **ifOperStatus** of the interface is not "up".
- **Show alarm when disconnected, but ignore when deactivated**: The sensor will turn into a **Down status**^[195] for a disconnected interface only if it is not deliberately deactivated in the configuration. This applies if the **ifOperStatus** of the interface is not "up" and the **ifAdminStatus** is "up". So the sensor will keep the **Up status**^[195] when the interface has been deactivated.
- **Ignore all "disconnected" states**: The sensor will not show an alarm and the **Up** status will persist.

 Monitoring will be discontinued without notice.

Alias Availability Shows if an alias is available for automatic **port name updates**^[416]. This value is shown for reference purposes only. We strongly

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.</p>
Chart Type	<p>Define how to show different channels for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> i You cannot use this option in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160]). Manual scaling is not possible if you choose this option. ▪ Show in and out traffic as positive and negative area chart: Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way. <ul style="list-style-type: none"> i You cannot use this option in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160]). Manual scaling is not possible if you choose this option. i You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the Sensor Channels Settings^[3160]).
Stack Unit	<p>This setting is only available if you choose Stack channels on top of each other above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

- | | |
|-------------------------|--|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ^[336] on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> |

SCANNING INTERVAL

- ❗ If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- ❗ Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- ❗ Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- ❗ To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none">▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below.▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies^[323] in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	<p>This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector^[240] to choose an object on which the current sensor will depend.</p>
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How do PRTG's automatic port name and number updates work for SNMP traffic sensors?

- <https://kb.paessler.com/en/topic/25893>

Knowledge Base: Where is the volume line in graphs?

- <https://kb.paessler.com/en/topic/61272>

Knowledge Base: Querying 64-bit Counters with SNMP Traffic Sensors

- <https://kb.paessler.com/en/topic/67503>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

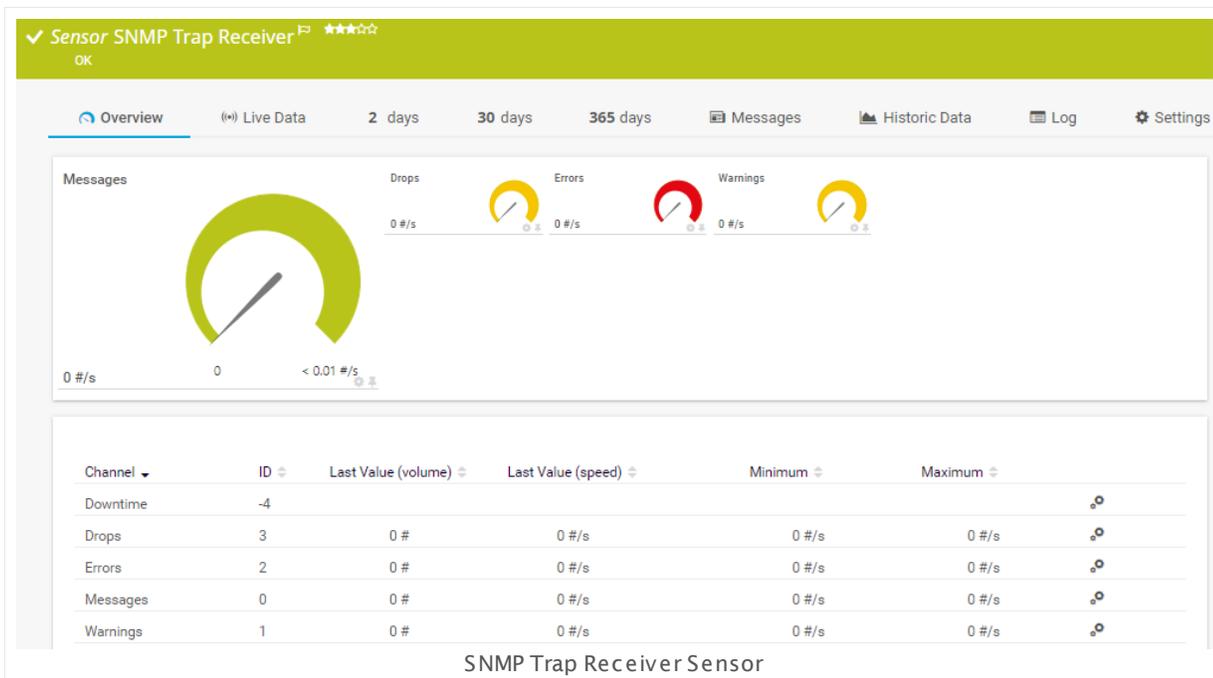
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.193 SNMP Trap Receiver Sensor

The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps.

It shows the following:

- Overall number of received traps per second
- Trap messages categorized as "warning" per second
- Trap messages categorized as "error" per second
- Number of dropped trap packets per second
- The actual trap messages



Sensor in Other Languages

Dutch: **SNMP Trap-ontvanger**, French: **Récepteur de trap SNMP**, German: **SNMP-Trap-Empfänger**, Japanese: **SNMP ? ? ? ? ? ?**, Portuguese: **Receptor de trap SNMP**, Russian: **Приемник ловушек SNMP**, Simplified Chinese: **SNMP ? ? ? ? ? ?**, Spanish: **Receptor SNMP Trap**

Remarks

- With the available filter options, you can define individually which types of messages the sensor will consider for monitoring, and which messages it will categorize as warning or error messages. Depending on the filters, received messages are counted in the respective channels.
- Add the sensor to the probe device to receive all messages of the system running the probe.

- Add the sensor to a specific device to receive all messages from this device directly. This makes this sensor type faster than just using source filters.
 - You can use specific placeholders in email [notification templates](#) ^[3316] to see the messages when you receive an email notification. See the Knowledge Base: [What placeholders can I use with PRTG?](#)
 - [Sensor states](#) ^[195] of this sensor type persist for one scanning interval only. If there is no warning or error message in the following scanning interval, the sensor will show an **up** status again. For a workaround, see this Knowledge Base article: [How can I configure sensors using speed limits to keep the status for more than one interval?](#)
 - If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - For a general introduction to the receiver's configuration, see manual section [Monitoring Syslogs and SNMP Traps](#) ^[3539].
 - This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
 - In PRTG on premises you can copy the Management Information Base (MIB) file for your traps into the [\MIB subfolder of your PRTG installation](#) ^[3731] to translate the OIDs for the traps into readable messages.
 - This sensor type does not support SNMP v3 traps! Please use SNMP v1 or v2c instead.
 - Knowledge Base: [How do I test an SNMP Trap Receiver Sensor?](#)
 - For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#) ^[3489].
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.
-  PRTG hosted by Paessler does not support the import of MIB files. The SNMP Trap Receiver sensor will only consider the MIBs that PRTG includes by default.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP TRAP SPECIFIC

Listen on Port	Enter the number of the port on which the sensor waits for SNMP traps. The default port is 162 . Please enter an integer value. We recommend that you use the default value.
Purge Messages After	Define for how long PRTG will store received trap messages for analysis. Choose a period of time from the dropdown list.

FILTER

Include Filter	<p>Define if you want to filter traps. If you leave this field empty or use the keyword "any", the sensor will process all data. This is the default setting. To include specific types of traps only, define filters using a special syntax.</p> <p> For more information, see section Filter Rules .</p>
Exclude Filter	<p>Define which types of traps the sensor will discard and not process. To exclude specific types of traps, define filters using a special syntax.</p> <p> For more information, see section Filter Rules .</p>
Warning Filter	<p>Define which types of traps count for the Warnings channel. To categorize received traps as warning messages, define filters using a special syntax.</p> <p> For more information, see section Filter Rules .</p> <p> Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Warning status  after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain Warning at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, its status will turn Up again after the interval.</p>
Error Filter	<p>Define which types of traps count for the Errors channel. To categorize received traps as error messages, define filters using a special syntax.</p> <p> For more information, see section Filter Rules .</p> <p> Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a Down status  after a scanning interval has finished and there was at least one error message during this interval. The status will remain Down at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, its status will turn Up again after the interval.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

DEBUGGING

Log Data to Disk Define if the probe will write a logfile of the received data to the data folder (see section [Data Storage](#)³⁷⁴) to the disk for debugging purposes. Choose between:

- **Off (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **On:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Traps

Filter rules are used for the include, exclude, warning, and error definition fields of the Trap Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which traps to monitor. Warning and error filters define how to categorize received traps. Provide these filters in the sensor settings as formulas. Formulas are fields that you can combine with boolean operators (**AND**, **OR**, **NOT**) and brackets.

FIELD	PARAMETER	EXAMPLES
source [ip]	Enter an IP address where the UDPs come from; IP masks and ranges are also possible.	source[10.0.23.50], source[10.0.23.10-50], source[10.0.23.10/255]
agent [ip]	Enter an IP address that specifies the object that creates the SNMP trap. Only v1 is supported.	agent[10.0.0.1]
enterprise [oid]	Enter an OID that specifies the object that originates the trap. Only v1 is supported.	enterprise [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0]
bindings [text]	Enter a substring to match all OIDs and values in the bindings.	bindings[ERROR], bindings [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0], bindings["port blocked"]
<p>i It is not necessary to use quotation marks (") to find strings, they will be internally removed.</p>		
bindings [oid,value]	Enter an OID and a substring to match a value in the given OID. Separate OID and value with a comma.	bindings [1.3.6.1.4.1.2.6.182.1.2.3 1.1.0,error]
gentrap [number]	Enter a number that specifies the generic trap type. Ranges are also possible.	gentrap[3], gentrap[2-6]
spectrap [number]	Enter a number that defines the specific trap code. Ranges are also possible.	spectrap[4], spectrap[0-3]
version [number]	Enter a number (1 or 2) that specifies the SNMP version.	version[1], version[2]
community [text]	Enter a community string for exact, case sensitive match.	community[public], community[private]

Messages Tab: Review and Analyze Traps

PRTG stores received traps as common files in the data folder (see section [Data Storage](#)). To review and analyze all received messages, you can access the most recent data directly in a [table list](#) in the PRTG web interface. You can access this list via the **Overview** tab of the sensors.

i Received traps are only shown after an (automatic) page refresh following to a sensor scan in the table on the **Overview** tab (default for [auto refresh](#) is 30 seconds).

For more details and further filter options, click the **Messages** tab of the SNMP Trap Receiver sensor. You will see all received messages in a [table list](#). On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG loads the filtered list automatically.

- ❶ Boolean operators are automatically applied to the filters in the following manner: the parameters across all columns are combined with **AND**, and the parameters within a single column are combined with **OR**.
- ❷ The parameters entered into the filters have to match **exactly** the parameters in the message. They are case sensitive!
- ❸ You can automatically add a filter by clicking the content of a column.

Advanced Filter Settings

You can open advanced filter settings with by clicking the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as described in section [Filter Rules for Traps](#)²⁴⁸⁸.

If you have provided filter parameters on the **Messages** tab, the advanced filter will already include them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Video Tutorial: How to Set Up an SNMP Trap Receiver Sensor in PRTG

- <https://www.paessler.com/support/videos/prtg-advanced/snmp-trap-receiver>

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

Knowledge Base: How do I test an SNMP Trap Receiver Sensor?

- <https://kb.paessler.com/en/topic/10193>

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

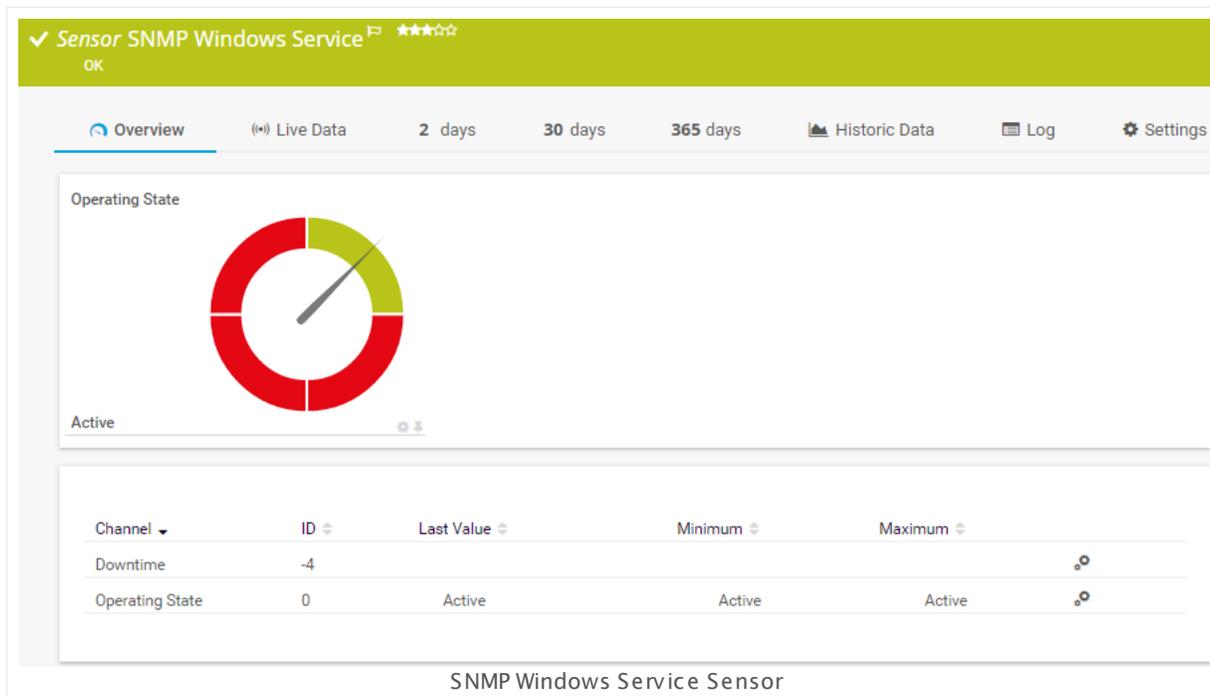
7.8.194 SNMP Windows Service Sensor

The SNMP Windows Service sensor monitors a Windows service via Simple Network Management Protocol (SNMP).

- It shows the operating status of the monitored service.

Operating states can be:

- Active ([sensor status](#)^[195] **Up**)
- Continue-Pending
- Pause-Pending
- Paused (all with sensor status **Down**)



Sensor in Other Languages

Dutch: **SNMP Windows Service**, French: **Service Windows SNMP**, German: **SNMP Windows-Dienst**, Japanese: **SNMP Windows** ? ? ? ? , Portuguese: **Serviço Windows SNMP**, Russian: **Служба Windows по SNMP**, Simplified Chinese: **SNMP Windows** ? ? , Spanish: **Servicio de Windows de SNMP**

Remarks

- This sensor type cannot distinguish the status "not installed" from "not running".
- It might not work to query data from a probe device via SNMP (querying `localhost`, `127.0.0.1`, or `:::1`). [Add this device to PRTG](#)^[31] with the IP address that it has in your network and create the SNMP sensor on this device instead.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].
- For a general introduction to the technology behind SNMP, please see the manual section [Monitoring via SNMP](#)^[3489].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Windows services you want to monitor. PRTG will create one sensor for each service you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SNMP WINDOWS SERVICE MONITOR

Service Select the services you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[219], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3252], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)

BASIC SENSOR SETTINGS



Parent Tags

Shows **Tags** that this sensor inherits from its parent device, group, and probe. This setting is shown for your information only and cannot be changed here.

Tags

Enter one or more **Tags**, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SNMP WINDOWS SERVICE MONITOR

Service

Shows the Windows service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[336] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

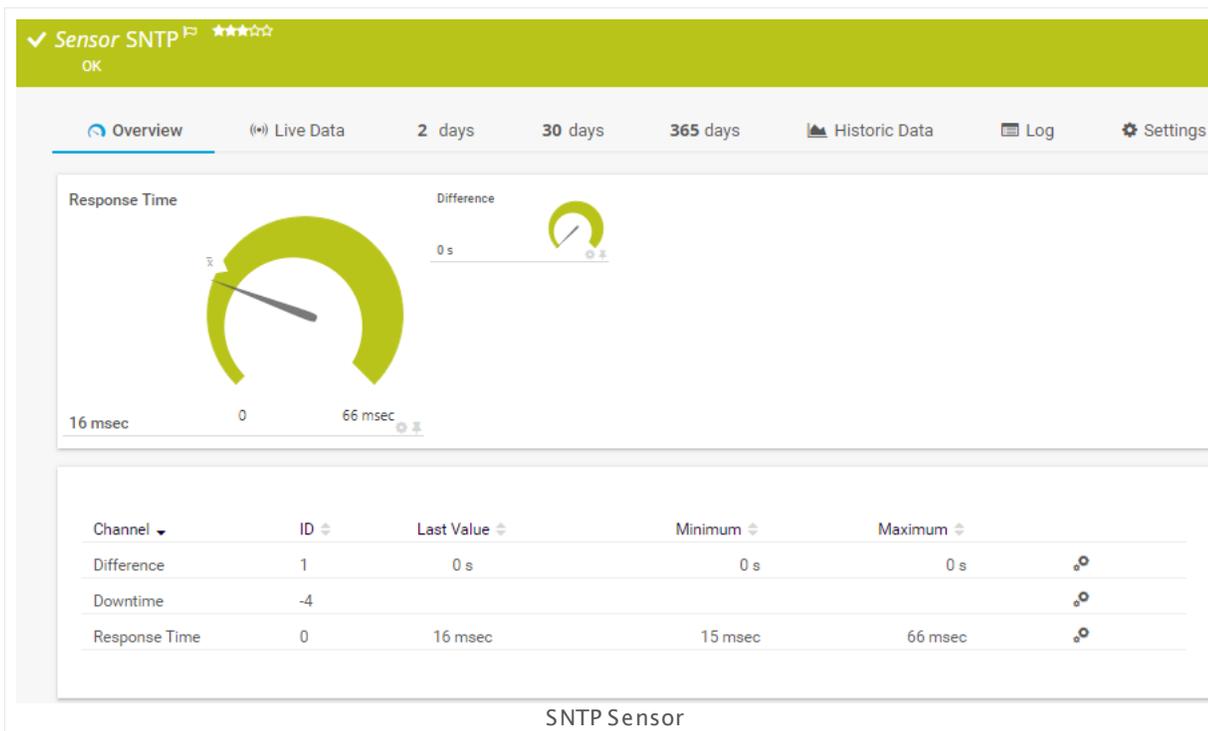
7.8.195 SNTP Sensor

The SNTP sensor monitors a Simple Network Time Protocol (SNTP) server.

It shows the following:

- Response time of the server
- Time difference in comparison to the local system time

The sensor tries to get a valid timestamp from the server up to three times per scan until it reports an error.



Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
----------------	--

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

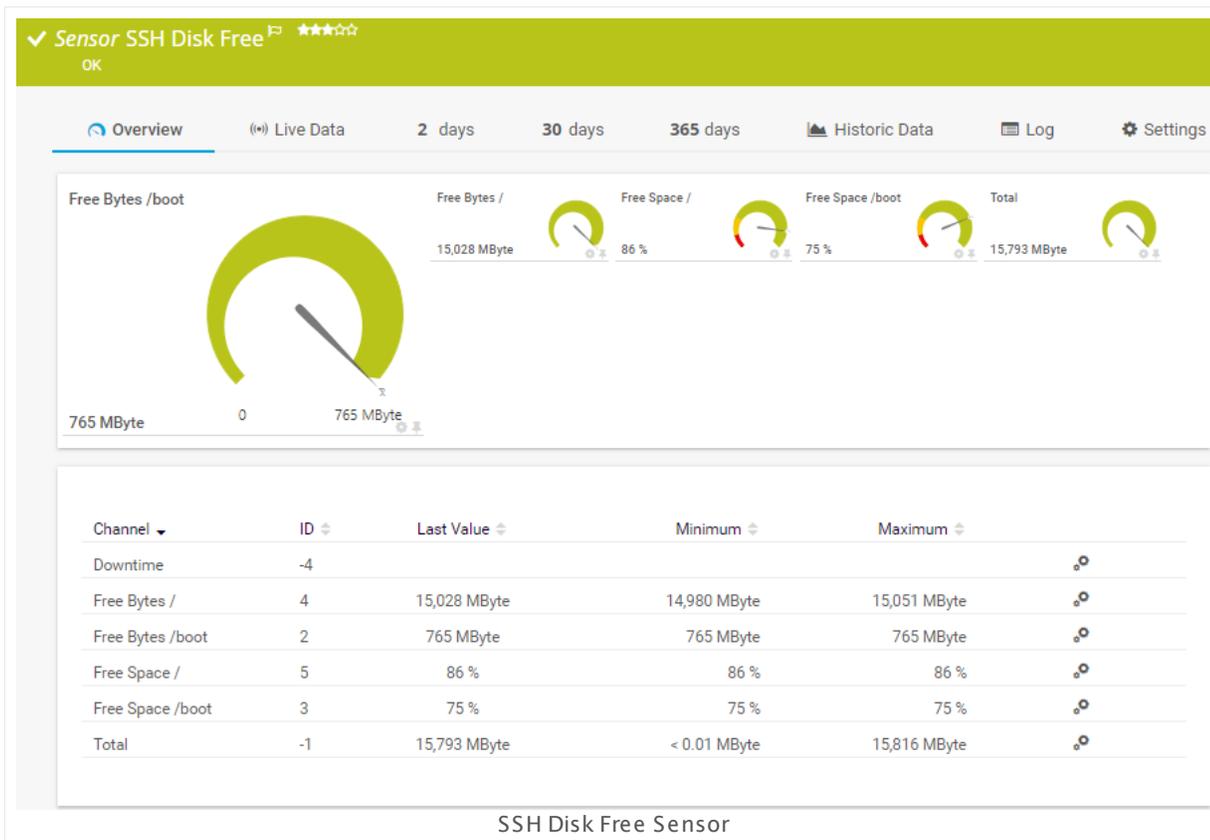
7.8.196 SSH Disk Free Sensor

The SSH Disk Free sensor monitors free space on disks of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Free disk space in bytes for every mounted partition
- Free disk space in percent for every mounted partition
- Total disk space

i The free space returned by this sensor type shows the available disk space of the volume, minus a reserve defined for this volume (for example, for redundancy purposes). So, this sensor shows the disk space that is actually available for use. The size of the reserved disk space can be defined with `tune2fs`. For details, see the Knowledge Base: [Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?](#)



Sensor in Other Languages

Dutch: **SSH Disk vrij**, French: **Espace disque disponible SSH**, German: **SSH Laufwerkskapazität**, Japanese: **SSH ? ? ? ? ? ? ? ?**, Portuguese: **SSH Disco livre**, Russian: **Свободное пространство диска по SSH**, Simplified Chinese: **SSH ? ? ? ? ? ? ? ?**, Spanish: **SSH disco libre**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#)³⁵¹⁰.
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disk(s) you want to monitor. PRTG will create two sensor channels (free space in percent and bytes) for each partition you choose in the **Add Sensor** dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH DISK FREE

Disk

Select the partitions that you want to monitor. You see a list with the names of all items that are available to monitor. Select the desired items by adding check marks in front of the respective lines. PRTG creates two channels for each selection. You can also select and deselect all items by using the check box in the table head.

i You can select up to 100 disks. If you select more disks, you will not be able to create the sensor. Add the sensor multiple times to monitor more than 100 disks with several sensors.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
---------------------------	--

SSH SPECIFIC

Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.</p>
SSH Port	<p>Define which port this sensor uses for the SSH connection. Choose between:</p> <ul style="list-style-type: none">▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems^[408] section of the device this sensor is created on.▪ Enter custom port number: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	<p>This field is only visible if you choose Enter custom port number above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.</p>
SSH Engine	<p>Select the method you want to use to access data with this SSH sensor^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p> <ul style="list-style-type: none">▪ Inherit from parent device (default): Use the SSH engine that you have defined in the parent device settings or higher in the object hierarchy^[133]. If you did not change it, this is the recommended default engine.▪ Default: This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the Inherit from parent device (default) option.▪ Compatibility Mode (deprecated): Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

 The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down status**¹⁹⁵, depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, please use the limit settings in the [Sensor Channels Settings](#)³¹⁶⁰.

 All limits that you define here are valid in addition to the limits defined in the particular **Channel** settings! The limits are valid simultaneously, so the first limit that is breached applies.

Percentage Limit Check Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between:

SET LIMITS CHECKED AGAINST ALL DISKS

- **Only use the limits in the settings of the percentage channels:** Do not define sensor limits that are valid for all percentage channels. The sensor only uses limits that you define in the settings of the particular "free space in percent" channels to determine the status.
- **Use the limits of both the sensor and the channel settings:** Define limits for the sensor that are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Warning Limit This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Warning** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Error Limit This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a **Down** status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

SET LIMITS CHECKED AGAINST ALL DISKS

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Size Limit Check

Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between:

- **Only use the limits in the settings of the byte size channels:** Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.
- **Use the limits of both the sensor and the channel settings:** Define limits for the sensor that are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will switch to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit

This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

- Lower Warning Limit** This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.
-  The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!
- Lower Error Limit** This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.
-  The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!
- Alarm on Missing/Removed Disk** If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between:
- **Deactivate alarm (default):** Select this option if you do not want an alarm for a removed disk.
 - **Activate alarm:** Select this option if you want to be alerted if a monitored disk is removed.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Knowledge Base: How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

Knowledge Base: Why do SSH Disk Free and SNMP Linux Disk Free show different values for my target Linux system?

- <https://kb.paessler.com/en/topic/43183>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

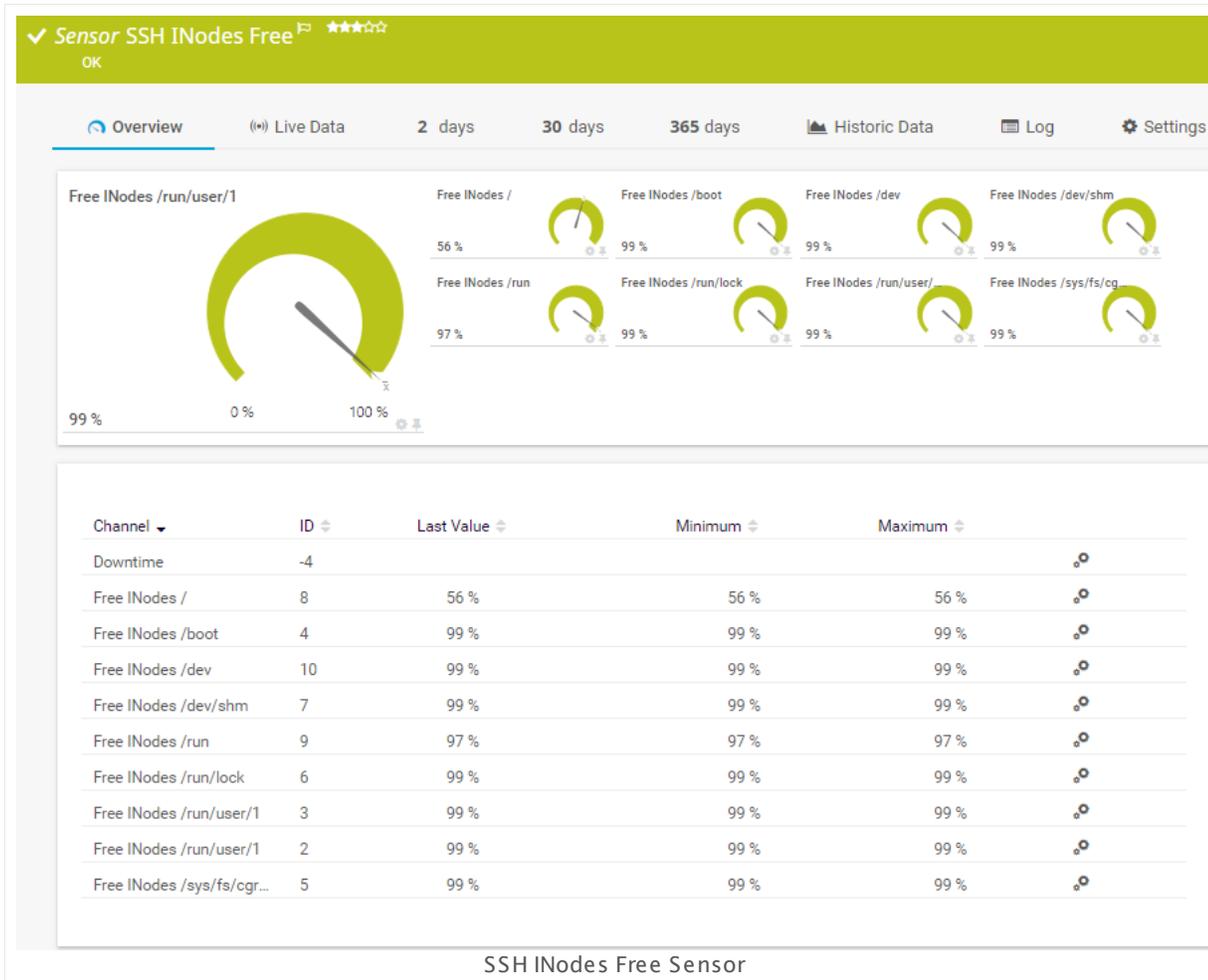
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.197 SSH INodes Free Sensor

The SSH INodes Free sensor monitors the free index nodes on disks of Linux/Unix and Mac OS systems via Secure Shell (SSH).

- It shows free index nodes in percent, for each mount in an individual sensor channel.

UNIX file systems only allow a limited number of index nodes. If the limit is exceeded, no more data can be stored, although there might still be free space available. This sensor can help you to notice early on if one of your drives is running out of INodes.



Sensor in Other Languages

Dutch: **SSH INodes Vrij**, French: **INodes SSH disponibles**, German: **SSH Freie INodes**, Japanese: **SSH I Nodes? ? ? ?**, Portuguese: **SSH INodes livre**, Russian: **Свободные узлы INodes по SSH**, Simplified Chinese: **SSH INode ? ? ? ?**, Spanish: **SSH INodes libres**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.

- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)
- This sensor type does not support ESX(i) hosts.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.) Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.

-  The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.
-  Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.

Shell Timeout (Sec.) Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, `cat /proc/loadavg`). The maximum value is **300** seconds (5 minutes). Please enter an integer value.

-  The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.
-  Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#) ⁴⁰⁸ section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

SSH SPECIFIC

Use Port Number This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine Select the method you want to use to [access data with this SSH sensor](#)³⁵¹⁰. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)¹³³. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

 The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.

SSH SPECIFIC

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Knowledge Base: How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

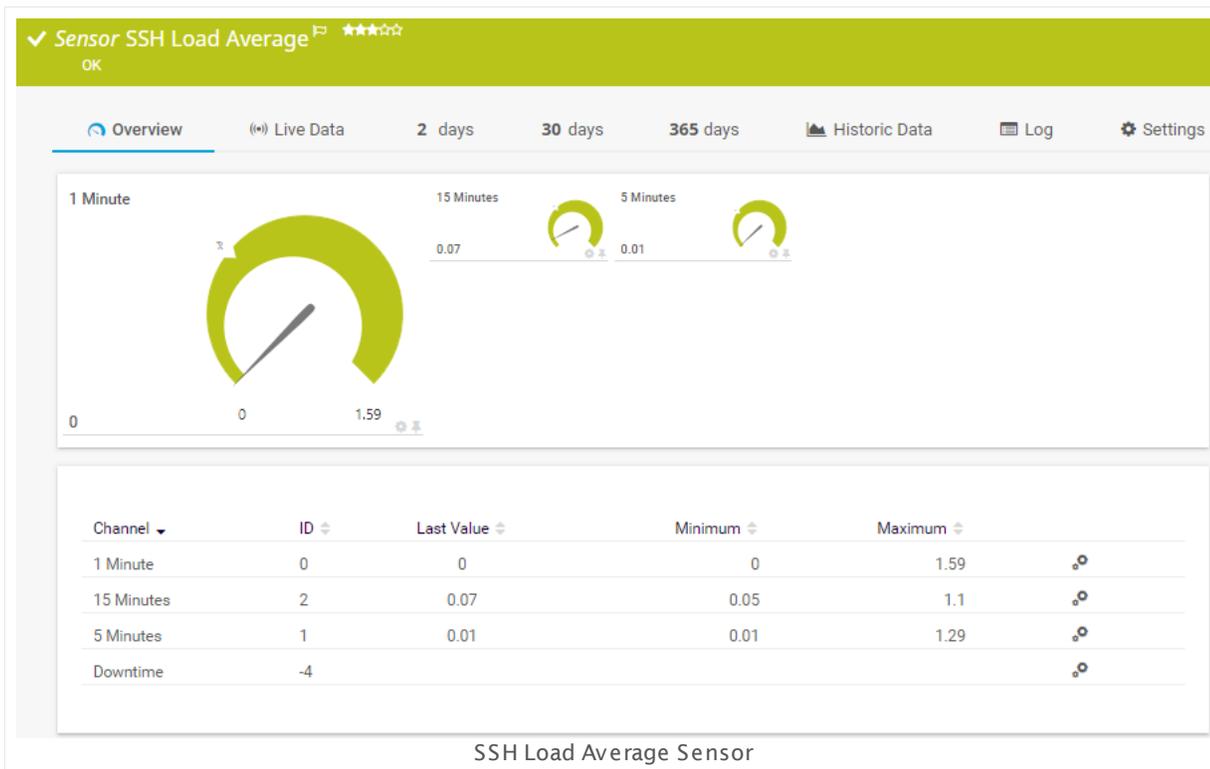
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.198 SSH Load Average Sensor

The SSH Load Average sensor monitors the load average of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Average system load within a 1-minute interval
- Average system load within a 5-minute interval
- Average system load within a 15-minute interval



Sensor in Other Languages

Dutch: **SSH Gemiddelde belasting**, French: **Moyenne de la charge SSH**, German: **SSH Durchschnitt l. Last**, Japanese: **SSH ? ? ? ? ? ? ? ?**, Portuguese: **SSH Carga média**, Russian: **Средняя загрузка по SSH**, Simplified Chinese: **SSH ? ? ? ? ?**, Spanish: **SSH carga promedio**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).

- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.</p>
SSH Port	<p>Define which port this sensor uses for the SSH connection. Choose between:</p> <ul style="list-style-type: none"> ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems^[408] section of the device this sensor is created on. ▪ Enter custom port number: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	<p>This field is only visible if you choose Enter custom port number above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.</p>
SSH Engine	<p>Select the method you want to use to access data with this SSH sensor^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p>

SSH SPECIFIC

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)¹³³. If you did not change it, this is the recommended default engine.
 - **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
 - **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.
-  The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Knowledge Base: How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷ section.

Others

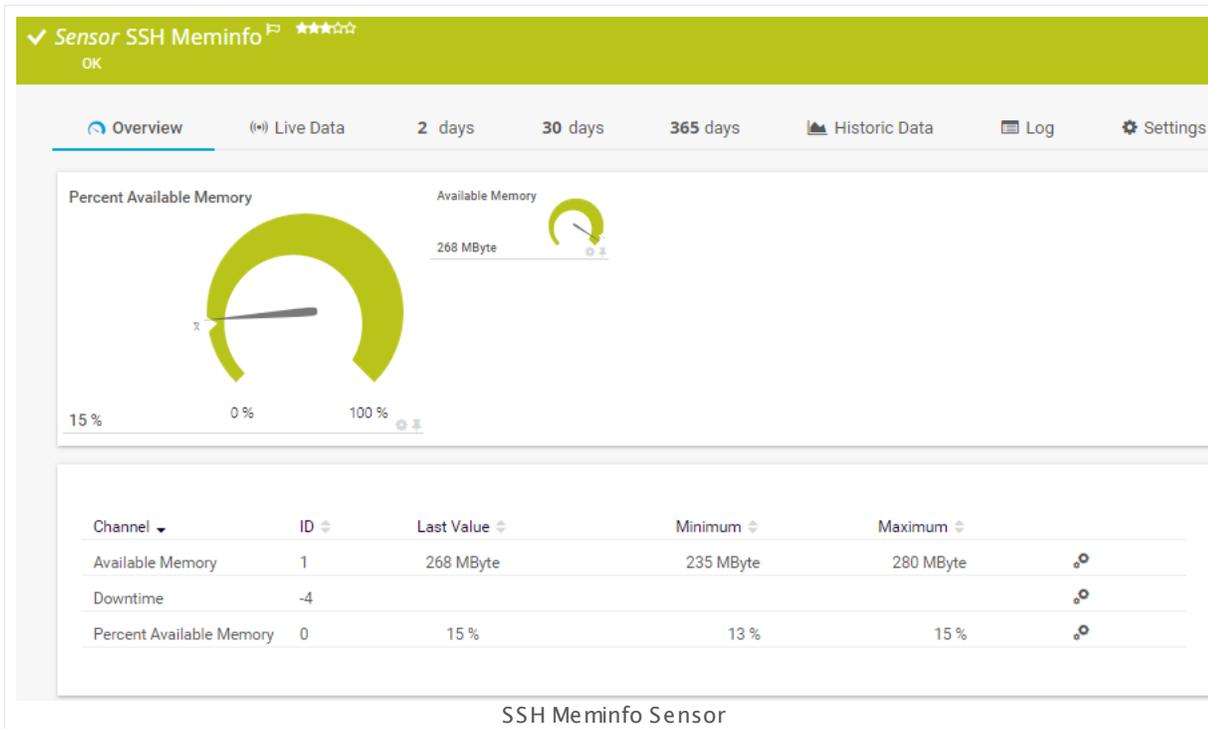
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.199 SSH Meminfo Sensor

The SSH Meminfo sensor monitors the memory usage of a Linux/Unix system using Secure Shell (SSH).

It shows the following:

- Available memory in bytes
- Available memory in percent



Sensor in Other Languages

Dutch: **SSH Meminfo**, French: **Info sur la mémoire SSH**, German: **SSH Speicherinfo**, Japanese: **SSH ? ? ? ? ?**, Portuguese: **SSH Meminfo**, Russian: **Meminfo no SSH**, Simplified Chinese: **SSH ? ? ? ? ?**, Spanish: **SSH información de memoria**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)
- This sensor type is not compatible with Mac OS systems.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.</p>
SSH Port	<p>Define which port this sensor uses for the SSH connection. Choose between:</p> <ul style="list-style-type: none"> ▪ Inherit port number from parent device (default): Use the port number as defined in the Credentials for Linux/Solaris/Mac OS (SSH/WBEM) Systems^[408] section of the device this sensor is created on. ▪ Enter custom port number: Define a custom port number below and do not use the port number from the parent device settings.
Use Port Number	<p>This field is only visible if you choose Enter custom port number above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.</p>
SSH Engine	<p>Select the method you want to use to access data with this SSH sensor^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:</p>

SSH SPECIFIC

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)¹³³. If you did not change it, this is the recommended default engine.
 - **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
 - **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.
-  The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Knowledge Base: How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

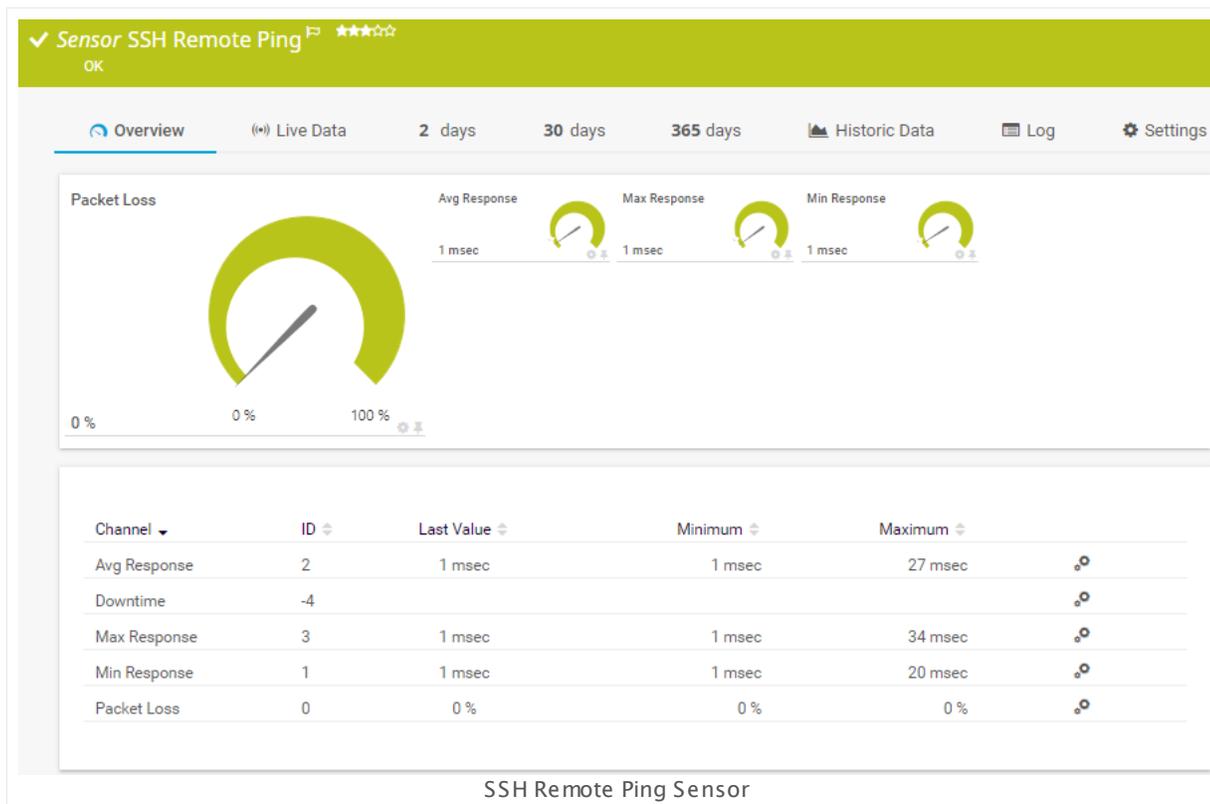
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.200 SSH Remote Ping Sensor

The SSH Remote Ping sensor remotely monitors the connectivity between a system running Linux/OS X and another device, using Internet Control Message Protocol (ICMP) echo requests (Ping) and Secure Shell (SSH).

It can show the following:

- Packet loss in percent
- Minimum, maximum, and average response times measured from the remote device you connect to



Sensor in Other Languages

Dutch: **SSH Remote Ping**, French: **Ping distant SSH**, German: **SSH Remote Ping**, Japanese: **SSH ? ? ? ? PING? ?**, Portuguese: **SSH Ping remoto**, Russian: **Удаленная проверка связи по SSH**, Simplified Chinese: **SSH? ? Ping**, Spanish: **Ping remoto SSH**

Remarks

- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).

- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH REMOTE PING CONFIGURATION

Target	Enter the DNS name or IP address of the target device the ping is sent to. The sensor will remotely connect to the parent device it is created on via SSH, then perform a ping request from this remote device to the target device or server. Please enter a string.
Packet Size (Bytes)	Enter the packet size in bytes for the ping. You can choose any value between 1 and 10000 . Please enter an integer value. We recommend that you use the default value.
Packet Count	Enter the number of packets that is sent with each scanning interval.
Custom Parameter	<p>Optionally enter additional parameters that will be added at the end of the ping command. Please enter a string or leave the field empty.</p> <p> Do not use parameters that change the output format of the result to make sure it can still be parsed. You cannot enter another command here.</p>

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p>

SSH SPECIFIC

- ⚠ Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

- ⓘ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.

SSH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Knowledge Base: How do I set up SSH sensors with my AWS Linux instances?

- <https://kb.paessler.com/en/topic/79569>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

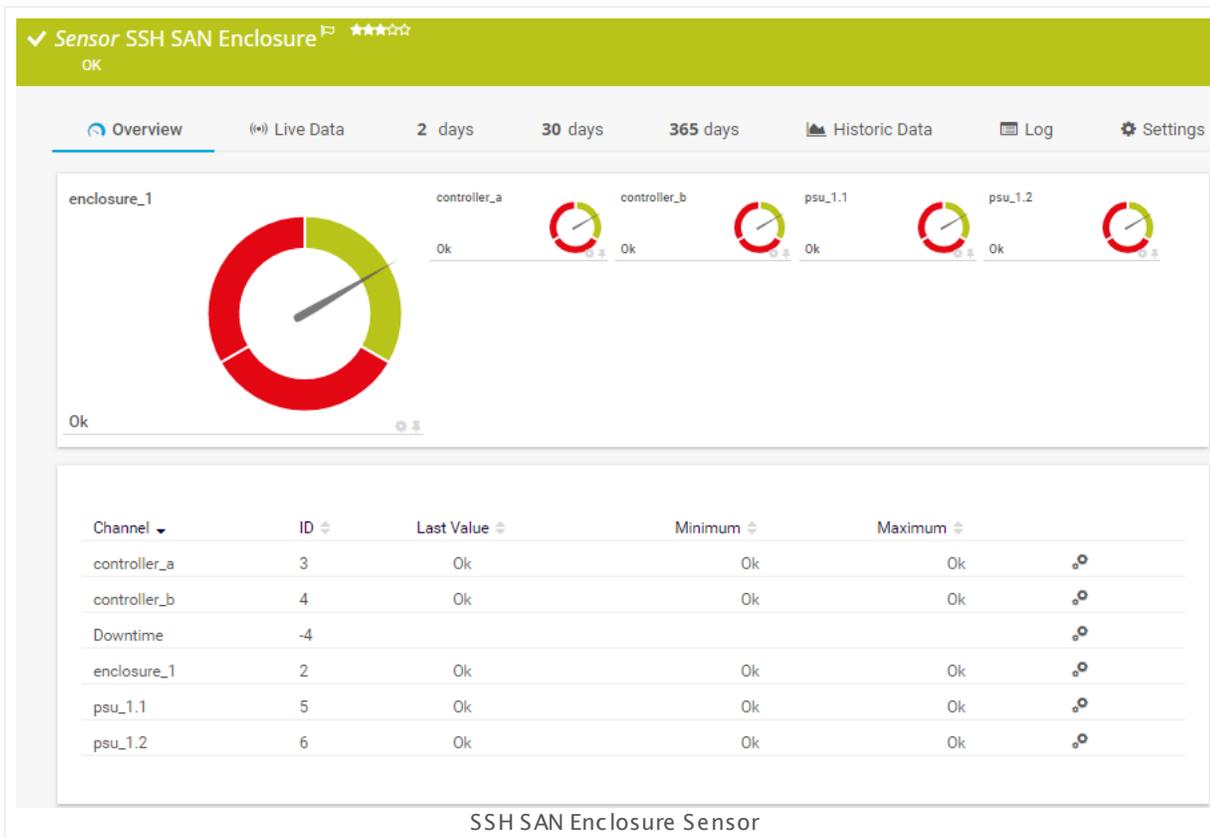
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.201 SSH SAN Enclosure Sensor

The SSH SAN Enclosure sensor monitors a Storage Area Network (SAN) enclosure via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Overall status of the enclosure
- Health status of the power supplies
- Health status of the controllers



Sensor in Other Languages

Dutch: **SSH SAN behuizing**, French: **Baie SAN SSH**, German: **SSH SAN Enclosure**, Japanese: **SSH SAN** , Portuguese: **SSH SAN Enclosure**, Russian: **Копнyc SAN нo SSH**, Simplified Chinese: **SSH SAN** , Spanish: **Carcasa de SAN de SSH**

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information on this issue, please see the Knowledge Base: [Why does my SSH SAN sensor show a wrong status?](#)
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[402] you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the [Monitoring via SSH](#)^[3510] section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the SAN enclosures you want to monitor. PRTG will create one sensor for each enclosure you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN ENCLOSURE SETTINGS

Enclosure	Select the enclosures you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-----------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SAN ENCLOSURE SETTINGS

Enclosure	Shows the identifier of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-----------	---

SSH SAN ENCLOSURE SETTINGS

Durable ID	Shows the durable identifier of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
WWN	Shows the WWN (World Wide Name) of the enclosure that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	<p>Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, cat /proc/loadavg). The maximum value is 300 seconds (5 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.</p>
SSH Port	Define which port this sensor uses for the SSH connection. Choose between:

SSH SPECIFIC

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

 The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.

SSH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

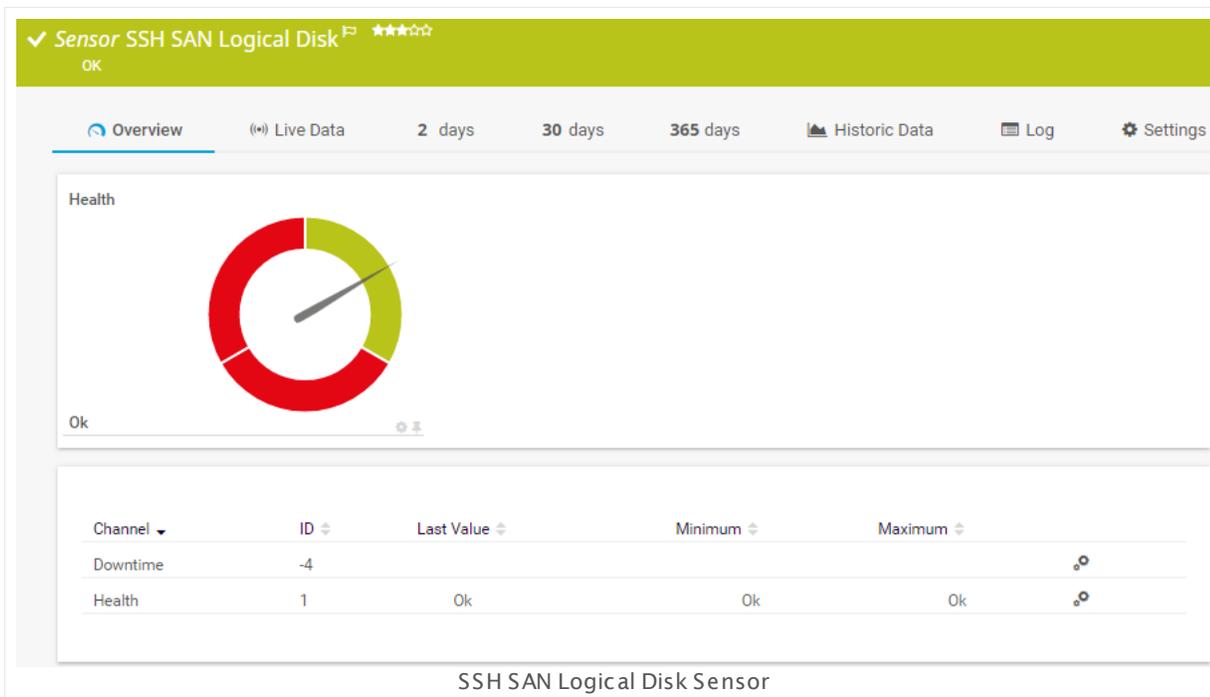
7.8.202 SSH SAN Logical Disk Sensor

The SSH SAN Logical Disk sensor monitors a logical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Health status of the disk
- Number of I/O operations per second
- Transferred data per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SSH SAN Logische Schijf**, French: **Disque logique SSH SAN**, German: **SSH SAN Logisches Laufwerk**, Japanese: **SSH SAN** ? ? ? ? ? ? , Portuguese: **SSH SAN Disco lógico**, Russian: **Логический диск SAN по SSH**, Simplified Chinese: **SSH SAN** ? ? ? ? , Spanish: **Disco lógico de SAN de SSH**

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.
- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.

- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information on this issue, please see the Knowledge Base: [Why does my SSH SAN sensor show a wrong status?](#)
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[402] you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the [Monitoring via SSH](#)^[3510] section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volumes on the SAN device you want to monitor. PRTG will create one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN LOGICAL DISK SETTINGS

Volume	Select the volumes you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
---------------------------	--

SSH SPECIFIC

Shell Timeout (Sec.) Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, `cat /proc/loadavg`). The maximum value is **300** seconds (5 minutes). Please enter an integer value.

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

 Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

SSH SPECIFIC

 The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SSH SAN LOGICAL DISK SETTINGS

Volume

Shows the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Size

Shows the size of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Command Mode

Define the command set to use on the monitored device to get monitoring data. Choose between:

SSH SAN LOGICAL DISK SETTINGS

- **Basic (recommended):** We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios.
- **Advanced:** This command set enables you to monitor additional data on the target device like IOs and bandwidth. Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you choose this option only if this data is crucial for your monitored volume.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

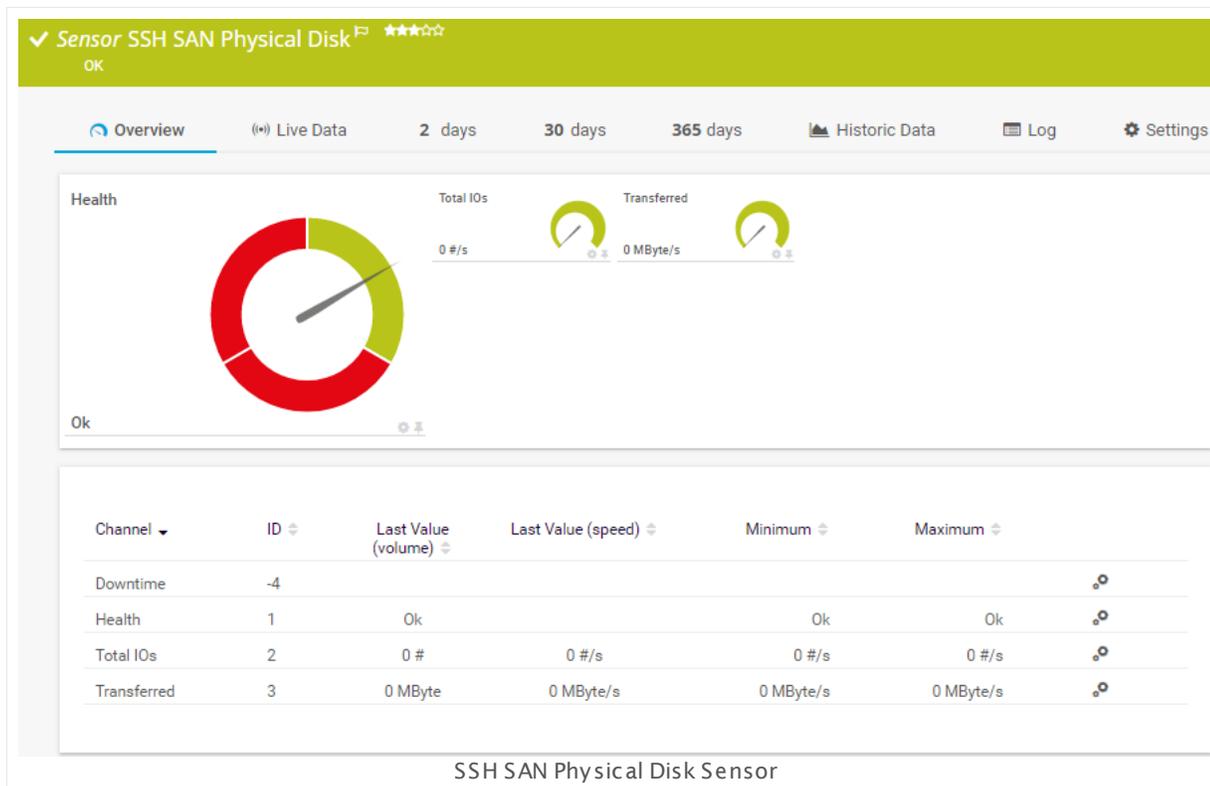
7.8.203 SSH SAN Physical Disk Sensor

The SSH SAN Physical Disk sensor monitors a physical disk on a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show the following:

- Health status of the disk
- Number of I/O operations per second
- Transferred data per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SSH SAN Fysieke Schijf**, French: **Disque physique SSH SAN**, German: **SSH SAN Physikalisches Laufwerk**, Japanese: **SSH SAN** ? ? ? ? ? , Portuguese: **SSH SAN Disco físico**, Russian: **Физический диск SAN по SSH**, Simplified Chinese: **SSH SAN** ? ? ? ? , Spanish: **Disco físico de SAN de SSH**

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.

- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information on this issue, please see the Knowledge Base: [Why does my SSH SAN sensor show a wrong status?](#)
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[402] you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the [Monitoring via SSH](#)^[3510] section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the disks on the SAN device you want to monitor. PRTG creates one sensor for each disk you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN PHYSICAL DISK SETTINGS

Disk	Select the disks you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SPECIFIC

Connection Timeout (Sec.)	<p>Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value.</p> <p>i The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p>
---------------------------	--

SSH SPECIFIC

- ⚠ Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.

Shell Timeout (Sec.)

Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, `cat /proc/loadavg`). The maximum value is 300 seconds (5 minutes). Please enter an integer value.

- ℹ The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

- ⚠ Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.

SSH SPECIFIC

- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.
- ❗ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SSH SAN PHYSICAL DISK SETTINGS

Disk

Shows the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SSH SAN PHYSICAL DISK SETTINGS

Disk Name	Shows the label of disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size	Shows the size of the disk that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Command Mode	Define the command set to use on the monitored device to get monitoring data. Choose between: <ul style="list-style-type: none">▪ Basic (recommended): We recommend that you use the basic command set for best sensor performance. This setting is appropriate for most scenarios.▪ Advanced: This command set enables you to monitor additional data on the target device like IOs and bandwidth. Because this setting results in higher usage of system resources and so might cause sensor instabilities, we strongly recommend that you choose this option only if this data is crucial for your monitored volume.

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.
Graph Type	Define how different channels will be shown for this sensor. <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

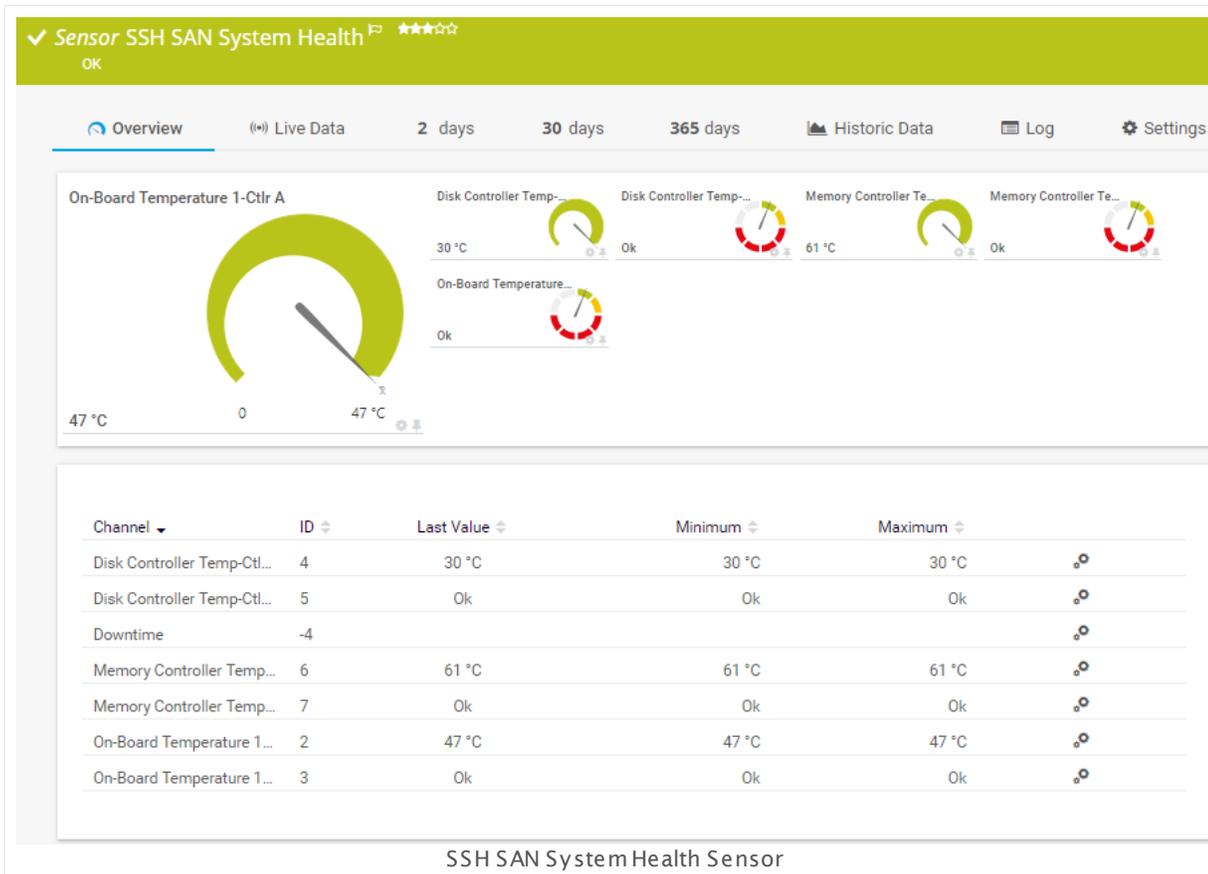
7.8.204 SSH SAN System Health Sensor

The SSH SAN System Health sensor monitors the system health of a Storage Area Network (SAN) via Secure Shell (SSH). The SAN has to provide a command-line interface (CLI) for this purpose.

It can show several metrics of an SAN, depending on the available measurement components on the SAN:

- Overall unit status
- Temperature and temperature states
- Voltage and voltage states
- Capacitor charge and status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **SSH SAN systeemstatus**, French: **L'état du système SSH SAN**, German: **SSH SAN Systemzustand**, Japanese: **SSH SAN ? ? ? ? ? ? ?**, Portuguese: **SSH SAN Funcionamento do sistema**, Russian: **Работоспособность системы SAN по SSH**, Simplified Chinese: **SSH SAN ? ? ? ?**

?? , Spanish: **Estado del sistema de SAN de SSH**

Remarks

- This sensor type does not support every SAN, even if it provides a CLI. The sensor only works with specific devices, for example, with the HP P2000.
- It may happen that the controller of your target device breaks down. The experience shows that this issue strongly depends on the hardware model you monitor. Please increase the scanning interval to discharge the controller and try again.
- Sometimes the devices you monitor with this SSH SAN sensor return status values that are not officially documented so that the shown sensor status in PRTG differs from the "real" device status. For more information on this issue, please see the Knowledge Base: [Why does my SSH SAN sensor show a wrong status?](#)
- After a firmware update of the target device, this sensor might show incorrect channel values. Please add this sensor type anew in this case.
- For this sensor type, you must define corresponding credentials in section **Credentials for Linux/Solaris/Mac OS (SSH/WBEM) System** in the [settings of the device](#)^[402] you want to use the sensor on.
- For a general introduction to SSH monitoring, please see the [Monitoring via SSH](#)^[3510] section.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)^[3693].

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the metrics you want to monitor. PRTG will create one sensor for each metric you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SSH SAN SPECIFIC

Metric	Select the metrics you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSH SAN SPECIFIC

Metric	Shows the metric this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
--------	---

SSH SAN SPECIFIC

Monitoring Mode

Define how the sensor requests data from the target device. The required mode depends on the firmware version of the device. Usually, the sensor automatically detects the firmware version and uses the appropriate mode. If you get errors, please explicitly define the firmware version.

Choose between:

- **Automatic Detection:** The sensor automatically detects the firmware version and uses the appropriate mode. We recommend that you use this option and only define the firmware date explicitly if you get errors.
- **Firmware prior to June 2015:** The sensor uses the mode that is appropriate for firmware versions dated before June 2015.
- **Firmware from June 2015 or later:** The sensor uses the mode that is appropriate for firmware versions dated from June 2015 or later.

We recommend that you use the default value.

SSH SPECIFIC

Connection Timeout (Sec.)

Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

 Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.

Shell Timeout (Sec.)

Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, `cat /proc/loadavg`). The maximum value is **300** seconds (5 minutes). Please enter an integer value.

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

SSH SPECIFIC

- ⚠ Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

- ⓘ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.

SSH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Why does my SSH SAN sensor show a wrong status?

- <https://kb.paessler.com/en/topic/60145>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

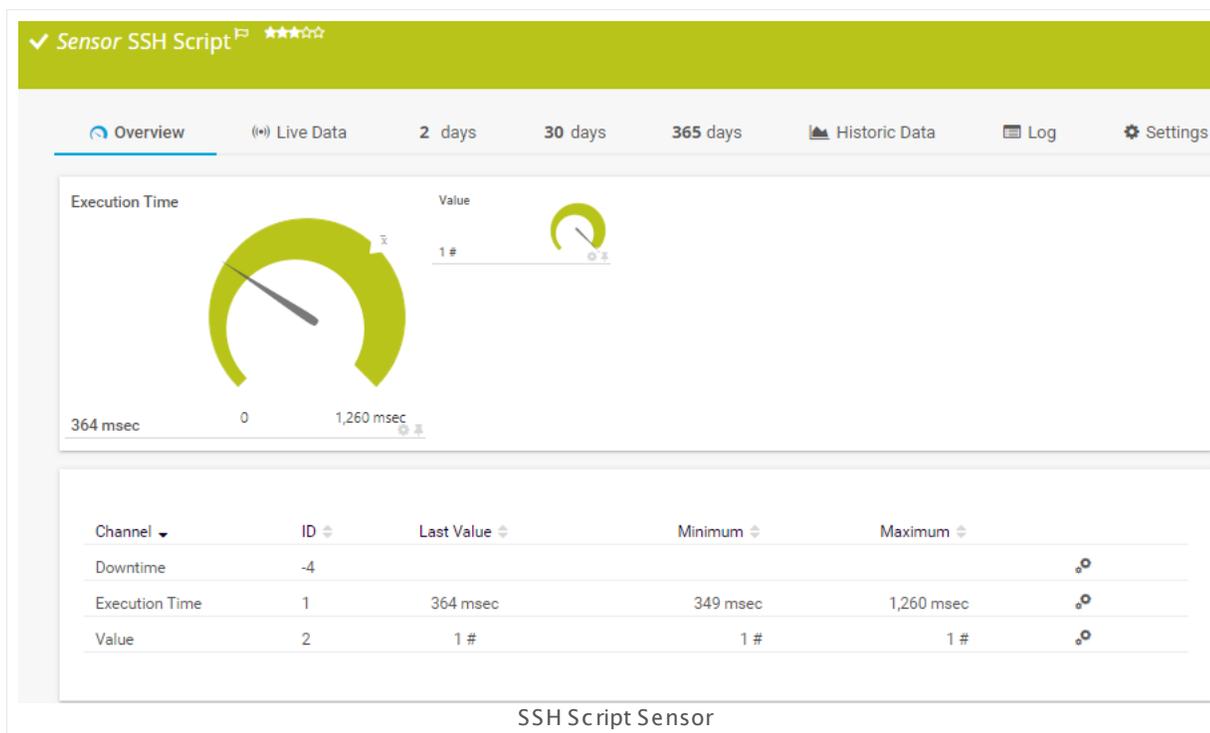
7.8.205 SSH Script Sensor

The SSH Script sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. This option is provided as part of the PRTG Application Programming Interface (API).

It shows the following:

- Execution time
- One value returned by the executable file or script (in one channel only).

 For details about the return value format, see section [Custom Sensors](#) .



Sensor in Other Languages

Dutch: **SSH Script**, French: **Script SSH**, German: **SSH-Skript**, Japanese: **SSH ? ? ? ? ? ? ?**, Portuguese: **SSH Script**, Russian: **скрипт SSH**, Simplified Chinese: **SSH ? ?**, Spanish: **Secuencia de comandos de SSH**

Remarks

- For details about the return value format, see manual section [Custom Sensors](#) .
- For security reasons, you must store your script file on the target system. The file must be located in the directory `/var/prtg/scripts`. Ensure the script has executable rights. If the script is not available or was deleted from the script folder, you will get the error message **Script not found (237)**.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#).
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script

Select a script file from the list. The dropdown menu will list all script files available in the `/var/prtg/scripts` directory on the target Linux/Unix system. For a script file to appear in this list, store the target file into this directory. Ensure the script has executable rights.

To show the expected sensor value and [status](#), your file must use the correct format for the returned values. In this case it is `exitcode:value:message` to standard output `stdout`. The exit code determines the sensor status.

 For detailed information on the expected return format and on how to build custom sensors, see section [Custom Sensors](#).

 For an example script, see the Knowledge Base: [Is there a shell script example for PRTG's SSH Script Sensor?](#)

Value Type

Define the type of the values that your script returns. Choose between:

- **Integer:** The return values are from the type integer. If the script returns a float, PRTG will show the value `0`.

SENSOR SETTINGS

- **Float:** The return values are from the type float, with a dot (.) between pre-decimal position and decimal places. With this setting, the sensor will also display integer values unless they produce a buffer overflow.
- **Counter:** Your script returns varying integer values. PRTG will show the difference between the values of two sensor scans.
 - ❗ A counter **must** return an integer, float values are not supported.
 - ❗ This sensor type does not support string values.

Channel Name Enter a name for the channel in which the sensor shows returned values. Please enter a string. This is for display purposes only. You can change the name later in the sensor's [channel settings](#).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

❗ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Script Shows the name of the script that the sensor executes with each scan. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Character Encoding Define the character encoding you use in your script to correctly display the sensor message. Choose between:

- **UTF-8 (default)**
- **ASCII**

Parameters If your script file catches command line parameters, you can define them here. You can use placeholders as well.

 For a full list of all placeholders see section [Custom Sensors](#)³⁶⁵⁴.

Please enter a string or leave the field empty.

 You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section [Escape Special Characters and Whitespaces in Parameters](#)²⁶¹⁹ for details. In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings.

Mutex Name Define any desired mutex name for the process. PRTG will run all custom script sensors having the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running at the same time. Please enter a string or leave the field empty.

SENSOR SETTINGS

 For more information, see the Knowledge Base: [What is the Mutex Name in the PRTG EXE/Script Sensor settings?](#)

Unit String	Define a unit for the channel value. Please enter a string. This is for display purposes only and will be the default unit for a new channel. You can change the unit after sensor creation in the sensor's channel settings ³¹⁶⁰ .
Value Type	Shows the expected type of the returned value. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
If Value Changes	Define what this sensor will do when the sensor value changes. You can choose between: <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification ³¹⁷⁰ whenever the sensor value changes.

SSH SPECIFIC

Connection Timeout (Sec.)	Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is 900 seconds (15 minutes). Please enter an integer value. <p> The sensor types SSH SAN Enclosure, SSH SAN Logical Disk, SSH SAN Physical Disk, SSH SAN System Health have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.</p> <p> Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.</p>
Shell Timeout (Sec.)	Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, <code>cat /proc/loadavg</code>). The maximum value is 300 seconds (5 minutes). Please enter an integer value.

SSH SPECIFIC

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

 Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

 The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

SSH SPECIFIC

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📖 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Escape Special Characters and Whitespaces in Parameters

 You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ":", "_", "-", "=", and "/" outside of quoted strings.

 We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#)³⁶⁵⁵ for details.

More

Knowledge Base: Is there a shell script example for the PRTG SSH Script Sensor?

- <https://kb.paessler.com/en/topic/39513>

Information about custom scripts and executables

- [Custom Sensors](#)³⁶³⁷
- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵

Knowledge Base: What is the Mutex Name in the PRTG EXE/Script Sensor settings?

- <https://kb.paessler.com/en/topic/6673>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

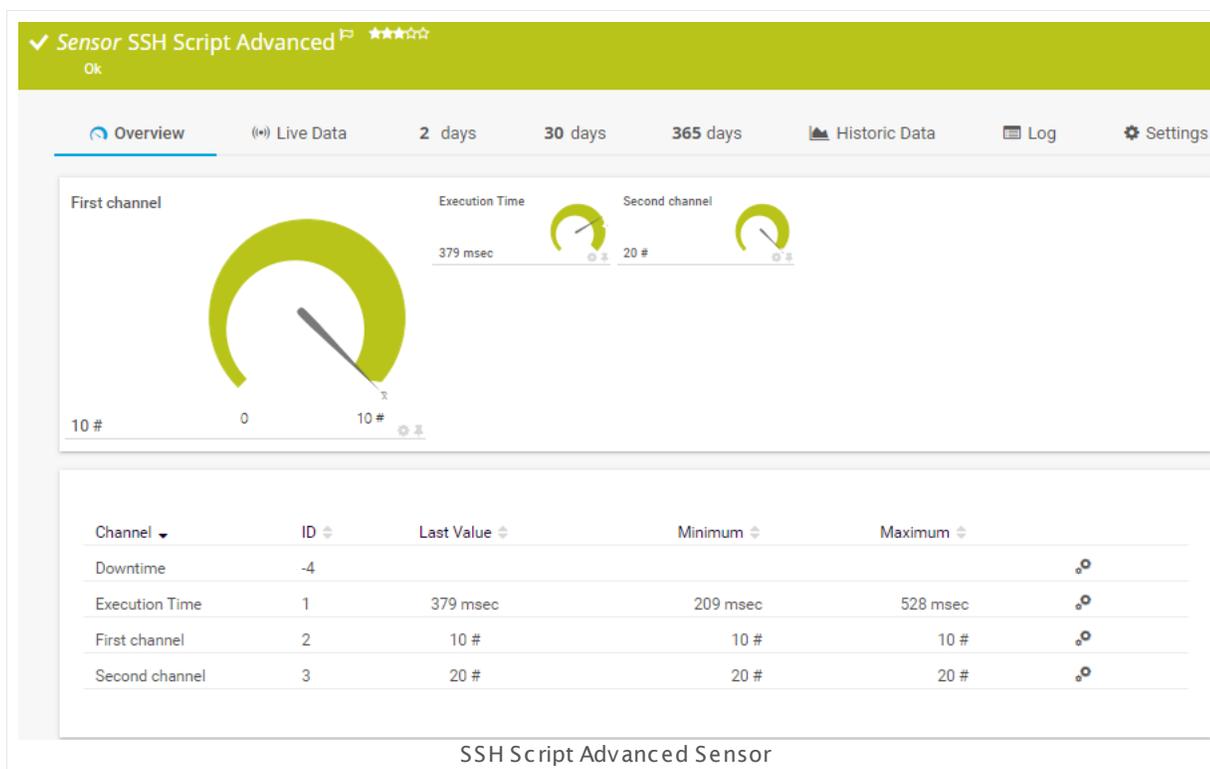
7.8.206 SSH Script Advanced Sensor

The SSH Script Advanced sensor connects to a Linux/Unix system via Secure Shell (SSH) and executes a script file located on the target system. This option is provided as part of the PRTG Application Programming Interface (API).

It can show the following:

- Execution time
- Values returned by the script in multiple channels. The return value of this sensor must be valid XML or JSON.

 For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.



Sensor in Other Languages

Dutch: **SSH Script Geavanceerd**, French: **Script SSH avancé**, German: **SSH-Skript (Erweitert)**, Japanese: **SSH ? ? ? ? ? (? ? ? ? ? ?)**, Portuguese: **SSH Script Avançado**, Russian: **Расширенный скрипт SSH**, Simplified Chinese: **?? SSH??**, Spanish: **Secuencia de comandos SSH avanzada**

Remarks

- For details about the return value format, see manual section [Custom Sensors](#)³⁶⁴¹.
- For security reasons, the script file must be stored on the target system. Make sure the script has executable rights.

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- This sensor type cannot support all Linux/Unix and Mac OS distributions.
- For a general introduction to SSH monitoring, please see manual section [Monitoring via SSH](#)³⁵¹⁰.
- Knowledge Base: [SSH and SFTP Sensors in Unknown Status](#)

Limited to 50 Sensor Channels

 PRTG does not support more than 50 sensor channels officially. Depending on the data used with this sensor type, you might exceed the maximum number of supported sensor channels. In this case, PRTG will try to display all sensor channels. However, please be aware that you will experience limited usability and performance.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Script

Select a script file from the list. The dropdown menu will list all script files available in the `/var/prtg/script/xml` directory on the target Linux/Unix system. For a script file to appear in this list, store the target file into this directory. Make sure the script has executable rights.

To show the expected sensor value and [status](#)¹⁹⁵, your files must return the expected XML or JSON format to standard output **stdout**. Values and message must be embedded in the XML or JSON.

 For detailed information on the expected return format and on how to build custom sensors, see section [Custom Sensors](#)³⁶⁴¹

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Script	Shows the script that the sensor executes with each scan. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Parameters	If your script file catches command line parameters, you can define them here. You can use placeholders as well.

SENSOR SETTINGS

 For a full list of all placeholders, see section [Custom Sensors](#)

Please enter a string or leave the field empty.

 You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section [Escape Special Characters and Whitespaces in Parameters](#) for details. In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings.

Mutex Name

Define any desired mutex name for the process. PRTG will execute all custom script sensors having the same mutex name serially (not simultaneously). This is useful if you use a lot of sensors and want to avoid high resource usage caused by processes running at the same time. Please enter a string or leave the field empty.

 For more information, see the Knowledge Base: [What is the Mutex Name in the PRTG EXE/Script Sensor settings?](#)

SSH SPECIFIC

Connection Timeout (Sec.)

Define a timeout in seconds for the connection. This is the time the sensor will wait to establish a connection to the host. Keep this value as low as possible. The maximum value is **900** seconds (15 minutes). Please enter an integer value.

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

 Ensure the connection timeout is a higher value than the shell timeout to avoid potential errors.

Shell Timeout (Sec.)

Define a timeout in seconds for the shell response. This is the time in seconds the sensor will wait for the shell to return a response after it has sent its specific command (for example, `cat /proc/loadavg`). The maximum value is **300** seconds (5 minutes). Please enter an integer value.

 The sensor types **SSH SAN Enclosure**, **SSH SAN Logical Disk**, **SSH SAN Physical Disk**, **SSH SAN System Health** have a fixed timeout of 300 seconds. Changing the value here will not have an effect on the timeout.

SSH SPECIFIC

- ⚠ Ensure the shell timeout is a lower value than the connection timeout to avoid potential errors.

SSH Port

Define which port this sensor uses for the SSH connection. Choose between:

- **Inherit port number from parent device (default):** Use the port number as defined in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#)^[408] section of the device this sensor is created on.
- **Enter custom port number:** Define a custom port number below and do not use the port number from the parent device settings.

Use Port Number

This field is only visible if you choose **Enter custom port number** above. Enter the port number (between 1 and 65535) that this sensor will use for the SSH connection. Please enter an integer value.

SSH Engine

Select the method you want to use to [access data with this SSH sensor](#)^[3510]. We strongly recommend that you use the default engine! For some time you still can use the legacy mode to ensure compatibility with your target systems. Choose between:

- **Inherit from parent device (default):** Use the SSH engine that you have defined in the parent device settings or higher in the [object hierarchy](#)^[133]. If you did not change it, this is the recommended default engine.
- **Default:** This is the default monitoring method for SSH sensors. It provides best performance and security. It is set by default in objects that are higher in the hierarchy so usually you can keep the **Inherit from parent device (default)** option.
- **Compatibility Mode (deprecated):** Try this legacy method only if the default mode does not work on a target device. The compatibility mode is the SSH engine that PRTG used in previous versions and is deprecated. We will remove this legacy option soon, so please try to get your SSH sensors running with the default SSH engine.

- ⓘ The option you select here overrides the selection of the SSH engine in a higher object (which is a parent device, group, probe, or root).

Result Handling

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.

SSH SPECIFIC

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt") in case of error:** Store the last result of the sensor only if it throws an error.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Escape Special Characters and Whitespaces in Parameters

 You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ":", "_", "-", "=", and "/" outside of quoted strings.

 We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#)³⁶⁵⁵ for details.

More

Information about custom scripts and executables

- [Custom Sensors](#)³⁶³⁷
- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵

Knowledge Base: What is the Mutex Name in the PRTG EXE/Script Sensor settings?

- <https://kb.paessler.com/en/topic/6673>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: How can I show special characters with EXE/Script sensors?

- <https://kb.paessler.com/en/topic/64817>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Knowledge Base: SSH and SFTP Sensors in Unknown Status

- <https://kb.paessler.com/en/topic/79174>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
206 SSH Script Advanced Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.207 SSL Certificate Sensor

The SSL Certificate sensor monitors the certificate of a secure Secure Sockets Layer (SSL)/Transport Layer Security (TLS) connection. It can show the following:

- Days to expiration with predefined lower warning limit (28 days) and lower error limit (7 days)
- Public key length
 - RSA keys: **Warning** [status](#)^[195] for 1024-bit keys (**Weak** security), **Up** status for 2048-bit keys (**Good** security) and longer (**Perfect** security); **Down** status for shorter keys (**Unsafe**)
 - ECC (Elliptic Curve Cryptography) keys: **Up** [status](#)^[195] for 128-bit and 192-bit keys (**Good** security) and longer (**Perfect** security); **Down** status for shorter keys (**Unsafe**)
- If common name or subject alternative names match the host address or SNI (if certificate name validation is enabled)
- If the certificate has been revoked (failing to query the certificate revocation list results in a warning status)
- If the certificate is trusted as root authority
- If the certificate is self-signed
- Certificate common name (sensor message)
- Certificate thumbprint (sensor message)

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

207 SSL Certificate Sensor

✓ **Sensor SSL Certificate Sensor** ★★★★☆

OK. Certificate Common Name: www.google.com - Certificate Thumbprint: F287312AF2E4D9A12D39DC99061ED3E1D577AC23

Overview Live Data 2 days 30 days 365 days Historic Data Log Settings

Last Scan: 12 s	Last Up: 12 s	Last Down:	Uptime: 100,0000%	Downtime: 0,0000%	Coverage: 100%	Sensor Type: SSL Certificate Sensor	Dependency: Parent	Interval: every 60 s	ID: #3987
-----------------	---------------	------------	-------------------	-------------------	----------------	-------------------------------------	--------------------	----------------------	-----------

Days to Expiration

64 0 64

Common Name Check	Public Key Length	Revoked	Root Authority Trusted
Disabled	Good (2048)	No	Yes
Self-Signed			
No			

Channel	ID	Last Value	Minimum	Maximum
Common Name Check	7	Disabled	Disabled	Disabled
Days to Expiration	2	64	64	64
Downtime	-4			
Public Key Length	5	Good (2048)	Good (2048)	Good (2048)
Revoked	4	No	Unable to check revocation...	No
Root Authority Trusted	3	Yes	Yes	Yes
Self-Signed	6	No	No	No

SSL Certificate Sensor

Sensor in Other Languages

Dutch: **SSL Certificaat Sensor**, French: **Capteur de certificat SSL**, German: **SSL-Zertifikatssensor**, Japanese: **SSL ? ? ? ? ? ?**, Portuguese: **Sensor do certificado SSL**, Russian: **Сенсор сертификата SSL**, Simplified Chinese: **SSL ? ? ? ? ?**, Spanish: **Sensor de certificado SSL**

Remarks

- Enter the DNS name in the parent [device settings](#)⁴⁰² exactly as written in your certificate. For example, enter **www.example.com** instead of **example.com**. The short version might not work properly with this sensor.
- To check the revocation status of a certificate, the sensor uses the same proxy settings as configured for the Windows user account on which the PRTG probe runs. This is usually the Windows local "system" user account. If you use a proxy, for example, please edit these settings in the Internet Explorer on this system accordingly (on the computer running the probe; on all nodes if in a cluster).
- This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#)³¹⁶⁰.

- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).
- ⓘ This sensor supersedes the deprecated HTTP Certificate Expiry sensor that is outdated.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSL CERTIFICATE SPECIFIC

Port Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is **443**.

Virtual Host (SNI Domain) Define the host name that the sensor will try to query if your server presents multiple certificates on the same IP address and port combination. Please enter a string.

In case of virtual hosting you need to identify the specific certificate for a specific domain while all domains use the same IP address, you can use Server Name Identification (SNI), which is an extension of Transport Layer Security (TLS).

i If you enable the **Common Name Validation** below, the sensor will compare the common name and optionally alternative names with the SNI defined here. Leave this field empty to validate the common name with the host address of the parent device.

Certificate Name Validation Define if you want the sensor to validate the certificate name. Choose between:

- **Do not compare common name with device address or SNI (default):** The sensor will not check if the certificate name is valid by comparing it with the address of the parent device or the defined SNI.
- **Compare and show 'down' status if common name and address/SNI do not match:** Check the common name to validate the certificate. If you set an SNI domain above, the sensor will compare the common name with this SNI. If you leave the SNI field empty, the sensor will use the host address of the parent device. If common name and the checked address/SNI do not match, the sensor will show a **Down status**¹⁹⁵.

SSL CERTIFICATE SPECIFIC

- **Compare and show 'down' status if common name/alternative names and address/SNI do not match:** Check common name and **Subject Alternative Names (SAN)** to validate the certificate. If you set an SNI domain above, the sensor will compare common name and alternative names with the SNI. If you leave the SNI field empty, the sensor will use the host address of the parent device. If common name or alternative names and the checked address/SNI do not match, the sensor will show a **Down status** ¹⁹⁵.

CONNECTION SPECIFIC

Use SOCKS Proxy (v5 only)

Define if you want to use a SOCKS proxy server for the sensor connection. Choose between:

- **Do not use SOCKS proxy (default):** The sensor will connect directly to the target host without using a SOCKS proxy.
- **Use SOCKS proxy:** The sensors will connect using **SOCKS5**. Provide data for the SOCKS connection below.

 Other SOCKS versions are not supported.

 This sensor type only supports SOCKS5 proxies. HTTP proxies are not supported.

SOCKS Proxy Server

This field is only visible if you choose **Use SOCKS proxy**. Enter the IP address or host name of the SOCKS5 proxy server that the sensor will use to connect.

SOCKS Proxy Server Port

This field is only visible if you choose **Use SOCKS proxy**. Enter the port number of the SOCKS5 proxy server that the sensor will use to connect.

SOCKS Proxy Server User

This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter a username.

SOCKS Proxy Server Password

This field is only visible if you choose **Use SOCKS proxy**. If the SOCKS5 proxy server requires authentication, enter the password for the user you specify above.

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

 You can use the debug option to get a logfile with information about the certificate chain. Additionally, certificates in the certificate chain are stored in the log folder (**.cer** files). This can help you, for example, if you have issues with the **Root Authority Trusted** channel of this sensor.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)^[336] on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[3383] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.208 SSL Security Check Sensor

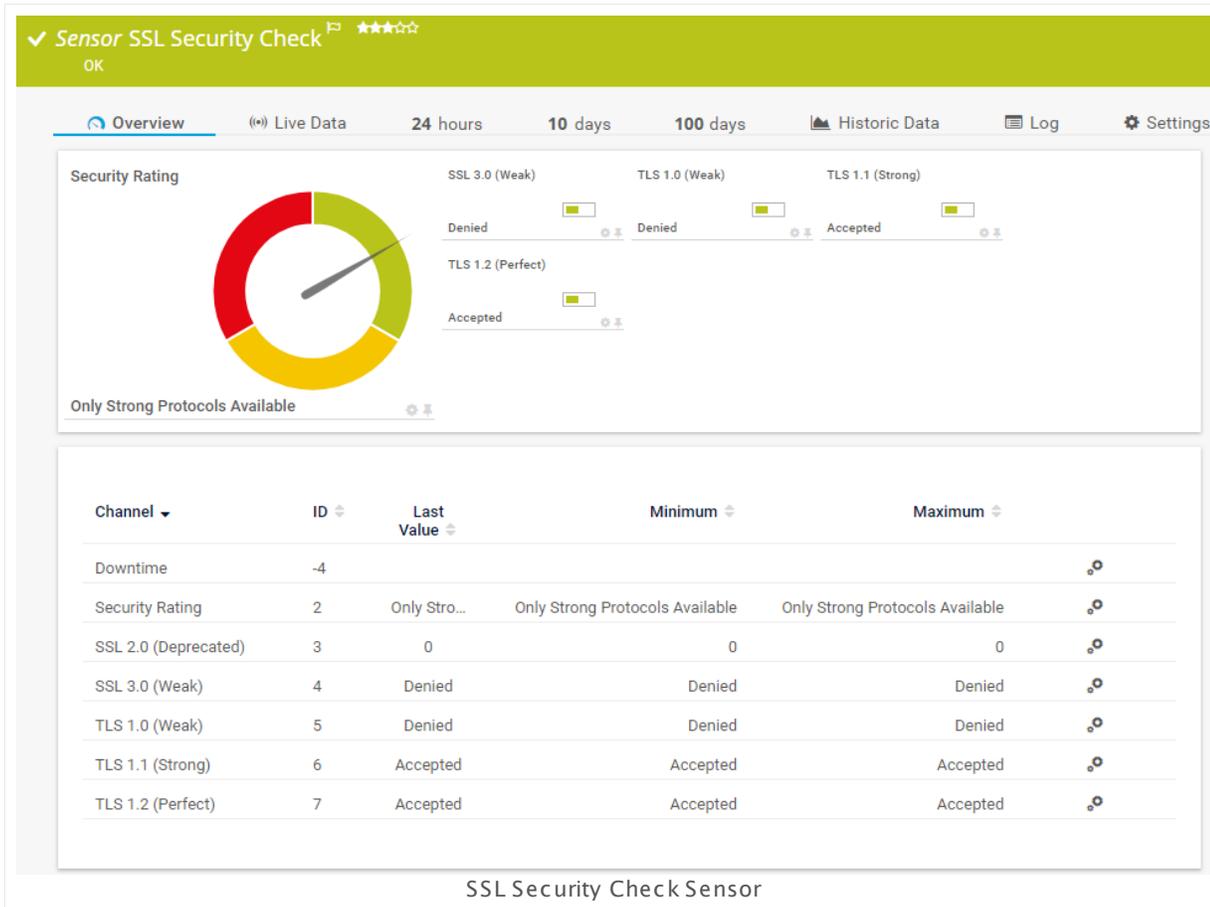
The SSL Security Check sensor monitors the Secure Sockets Layer (SSL) connectivity to the port of a device. It tries to connect to the specified TCP/IP port number of a device with various SSL/TLS protocol versions and shows if a particular protocol is supported.

The sensor checks connectivity with the following protocols in particular [channels](#)^[136] with the possible values **Accepted** (sensor can connect with this protocol) or **Denied** (sensor cannot connect with this protocol):

- **SSL 3.0:** weak security (warning if accepted, up if denied)
- **TLS 1.0:** weak security (warning if accepted, up if denied)
- **TLS 1.1:** strong security (up if accepted, otherwise gray)
- **TLS 1.2:** perfect security (up if accepted, otherwise gray)

The default primary channel **Security Rating** shows the connection security to the defined port with one of the following [states](#)^[195]:

- **Down:** There is no secure protocol available. The sensor cannot connect with one of the given protocols.
- **Warning (weak):** The sensor can connect with at least one of the weak protocols SSL 3.0, or TLS 1.0.
- **Up (strong):** The sensor can connect with a strong protocol only (TLS 1.1, TLS 1.2). Connecting with a weak protocol is not possible.



Sensor in Other Languages

Dutch: **SSL Security Check**, French: **Vérification de sécurité SSL**, German: **SSL-Sicherheit überprüfung**, Japanese: **SSL ? ? ? ? ? ? ? ? ?**, Portuguese: **Verificação de segurança SSL**, Russian: **Проверка безопасности SSL**, Simplified Chinese: **SSL ? ? ? ?**, Spanish: **Comprobación de seguridad SSL**

Remarks

- This sensor only checks accepted protocols, it does not consider the used ciphers.
- Knowledge Base: [How do you determine the protocol security ratings of the SSL Security Check sensor?](#)
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#).

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SSL SECURITY SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is 443 .
Virtual Host (SNI Domain)	Enter a host name that the sensor will query. The sensor uses this host to connect if the target server presents multiple certificates on the same IP address and IP port when using Server Name Identification (SNI).

CONNECTION SPECIFIC

Use SOCKS Proxy (v5 only)	<p>Define if you want to use a SOCKS proxy server for the sensor connection. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not use SOCKS proxy (default): The sensor will connect directly to the target host without using a SOCKS proxy. ▪ Use SOCKS proxy: The sensors will connect using SOCKS5. Provide data for the SOCKS connection below. <ul style="list-style-type: none"> ❗ Other SOCKS versions are not supported. ❗ This sensor type only supports SOCKS5 proxies. HTTP proxies are not supported.
SOCKS Proxy Server	This field is only visible if you choose Use SOCKS proxy . Enter the IP address or host name of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server Port	This field is only visible if you choose Use SOCKS proxy . Enter the port number of the SOCKS5 proxy server that the sensor will use to connect.
SOCKS Proxy Server User	This field is only visible if you choose Use SOCKS proxy . If the SOCKS5 proxy server requires authentication, enter a username.
SOCKS Proxy Server Password	This field is only visible if you choose Use SOCKS proxy . If the SOCKS5 proxy server requires authentication, enter the password for the user you specify above.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵⁵ on PRTG on premises installations.</p>
-------------------	---

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How do you determine the protocol security ratings of the SSL Security Check sensor?

- <https://kb.paessler.com/en/topic/71566>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

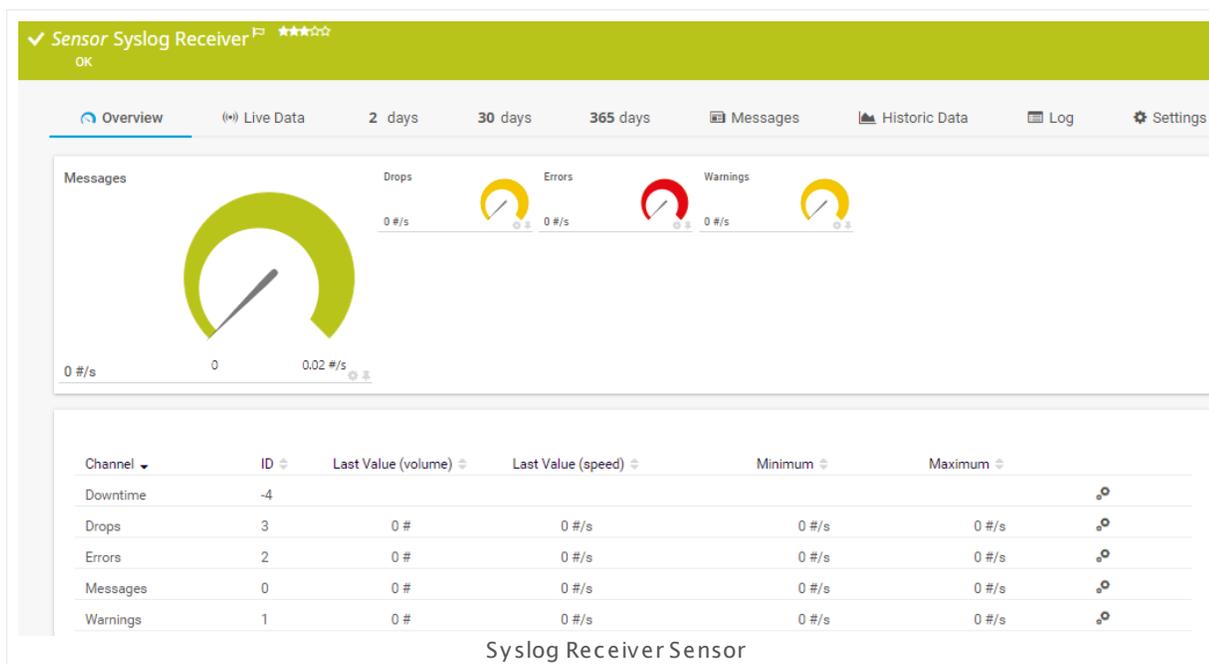
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.209 Syslog Receiver Sensor

The Syslog Receiver sensor receives and analyzes Syslog messages.

It shows the following:

- Number of received syslog messages per second
- Number of messages categorized as "warning" per second
- Number of messages categorized as "error" per second
- Number of dropped packets per second



Sensor in Other Languages

Dutch: **Syslog ontvanger**, French: **Récepteur Syslog**, German: **Syslog-Empfänger**, Japanese: **Syslog** ? ? ? ? ? , Portuguese: **Destinatário de syslog**, Russian: **Приемник Syslog**, Simplified Chinese: ? ? ? ? ? ? ? ? , Spanish: **Receptor Syslog**

Remarks

- With the available filter options, you can define individually which types of messages the sensor will consider for monitoring, and which messages it will categorize as warning or error messages. Depending on the filters, received messages are counted in the respective channels.
- Add the sensor to the probe device to receive all messages of the system running the probe.
- Add the sensor to a specific device to receive all messages from this device directly. This makes this sensor type faster than just using source filters.

- You can use specific placeholders in email [notification templates](#)^[3316] to see the messages when you receive an email notification. See the Knowledge Base: [What placeholders can I use with PRTG?](#)
 - [Sensor states](#)^[195] of this sensor type persist for one scanning interval only. If there is no warning or error message in the following scanning interval, the sensor will show an **up** status again. For a workaround, see this Knowledge Base article: [How can I configure sensors using speed limits to keep the status for more than one interval?](#)
 - If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.
 - This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.
 - For a general introduction to the receiver's configuration, see manual section [Monitoring Syslogs and SNMP Traps](#)^[3539].
 - This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SYSLOG SPECIFIC

Listen on Port	Enter the number of the port on which the sensor waits for Syslog messages. The default port is 514 . Please enter an integer value. We recommend that you use the default value.
Purge Messages After	Define how long PRTG stores received Syslog messages for analysis. Choose a period of time from the dropdown list.

FILTER

Include Filter Define if you want to filter Syslog messages. If you leave this field empty or use the keyword **any**, the sensor will process all data. To include specific types of messages only, define filters using a special syntax.

 For more information, see section [Filter Rules](#) .

Exclude Filter Define which types of Syslog messages the sensor will discard and not process. To exclude specific types of messages, define filters using a special syntax.

 For more information, see section [Filter Rules](#) .

Warning Filter Define which types of Syslog messages count for the **Warnings** channel. To categorize received messages as warning messages, define filters using a special syntax.

 For more information, see section [Filter Rules](#) .

 Messages are collected until a scanning interval ends. as long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Warning** status after a scanning interval has finished and there was at least one warning message (and no error message) during this interval. The status will remain **Warning** at least until the succeeding scanning interval has finished. If in this scanning interval no warning or error message occurred, the status of the sensor will turn **Up** again after the interval.

Error Filter Define which types of syslog messages will count for the **Errors** channel. To categorize received messages as error messages, define filters using a special syntax.

 For more information, see section [Filter Rules](#) .

 Messages are collected until a scanning interval ends. As long as the scanning interval is running, no status change will happen. By default, the sensor will turn into a **Down** status after a scanning interval has finished and there was at least one error message during this interval. The status will remain **Down** at least until the succeeding scanning interval has finished. If the sensor did not receive any warning or error message in this scanning interval, the status of the sensor will turn **Up** again after the interval.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

DEBUGGING

Log Data to Disk Define if the probe will write a logfile of the received data to the data folder (see [Data Storage](#)³⁷³⁴) to the disk for debugging purposes. Choose between:

- **Off (recommended):** Do not write additional logfiles. Recommended for normal use cases.
- **On:** Write logfiles for all data received.

 Use with caution! When enabled, huge data files can be created. Please use for a short time and for debugging purposes only.

Filter Rules for Syslog Messages

Filter rules are used for the include, exclude, warning, and error definition fields of the Syslog Receiver sensor. They are based on the following format:

```
field[filter]
```

You can use various filters suitable to your needs. Include and exclude filters define which messages to monitor. Warning and error filters define how to categorize received messages. Provide these filters in the sensor settings as formulas. Formulas are fields that you can combine with boolean operators (**AND**, **OR**, **NOT**) and brackets.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
209 Syslog Receiver Sensor

FIELD	PARAMETER	EXAMPLE
source [ip]	the IP address where the messages will be received from; masks and ranges are also possible	<ul style="list-style-type: none"> ▪ source[10.0.23.50] ▪ source[10.0.23.10-50] ▪ source[10.0.23.10/255]
facility [number]	any number or range from 0 to 23 specifying the type of program sending the message	<ul style="list-style-type: none"> ▪ facility[2] ▪ facility[5-7] ▪ facility[5] OR facility[6]
severity [number]	any number or range from 0 (emergency) to 7 (debug) specifying the type of message	<ul style="list-style-type: none"> ▪ severity[4] ▪ severity[1-3] ▪ severity[1] AND severity [2]
host name [text]	any string specifying the hostname of a device in the message	<ul style="list-style-type: none"> ▪ hostname [www.example.com]
tag [text]	any string specifying the tag of a program or process in the message	<ul style="list-style-type: none"> ▪ tag[su]
appname [text]	any string specifying the appname part of the message	<ul style="list-style-type: none"> ▪ appname[myproc] ▪ appname[demo] AND msgid[m42]
procid [text]	any string specifying the process identifier part of the message	<ul style="list-style-type: none"> ▪ procid[1860]
msgid [text]	any string specifying the message identifier part of the message	<ul style="list-style-type: none"> ▪ msgid[ID47]
message [parttext]	any string specifying the message part of the message (substring will match; case insensitive!)	<ul style="list-style-type: none"> ▪ message[Error]
data [id ,param,value]	checks the SD-ID block of the message's structured data for a parameter matching the given value	<ul style="list-style-type: none"> ▪ data [exampleSDID@12345,eventSource,Application]
data [parttext]	checks if the given substring matches on structured data as displayed in the corresponding table	<ul style="list-style-type: none"> ▪ data [exampleSDID@1234]
data [id,param]	checks if the parameter exists in the given ID element	<ul style="list-style-type: none"> ▪ data [exampleSDID@1234,eventSource]

- ❗ String parameters (except the substring in **message**) have to match **exactly** the particular parts of the message. They are case sensitive!

Messages Tab: Review and Analyze Syslog Messages

PRTG stores received Syslog messages as common files in the data folder (see section [Data Storage](#)³⁷³⁴). To review and analyze all received messages, you can access the most recent data directly in a [table list](#)²³⁷ in the PRTG web interface. You can access this list via the **Overview** tab of the sensors.

- ❗ Received syslog messages are only shown after an (automatic) page refresh following to a sensor scan in the table on the **Overview** tab (default for [auto refresh](#)³³⁰⁴ is 30 seconds).

For more details and further filter options, click the **Messages** tab of the Syslog Receiver sensor. You will see all received messages in a [table list](#)²³⁷. On the top, you have display filter options to drill down into the data for specific events of your interest. The filters are the same as available in the sensor settings, but you can define them without using formulas. Provide the desired parameters and PRTG loads the filtered list automatically.

- ❗ You can automatically add a filter by clicking the content of a column.

Advanced Filter Settings

You can open advanced filter settings by clicking the gear icon in the **Filter** row. The **Advanced Filter** will appear in a popup window. In the text field, you can define a filter using the syntax as given in section [Filter Rules for Syslog Messages](#)²⁶⁶⁵.

If you have provided filter parameters on the **Messages** tab, the advanced filter will already include them as a corresponding formula with the correct syntax. You can adjust this filter to your needs. You can also copy the automatically created and manually adjusted formula for usage in the filter fields of the sensor settings.

More

Video Tutorial: Create and Configure a Syslog Receiver Sensor in PRTG

- <https://www.paessler.com/support/videos/prtg-advanced/syslog-receiver>

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
209 Syslog Receiver Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

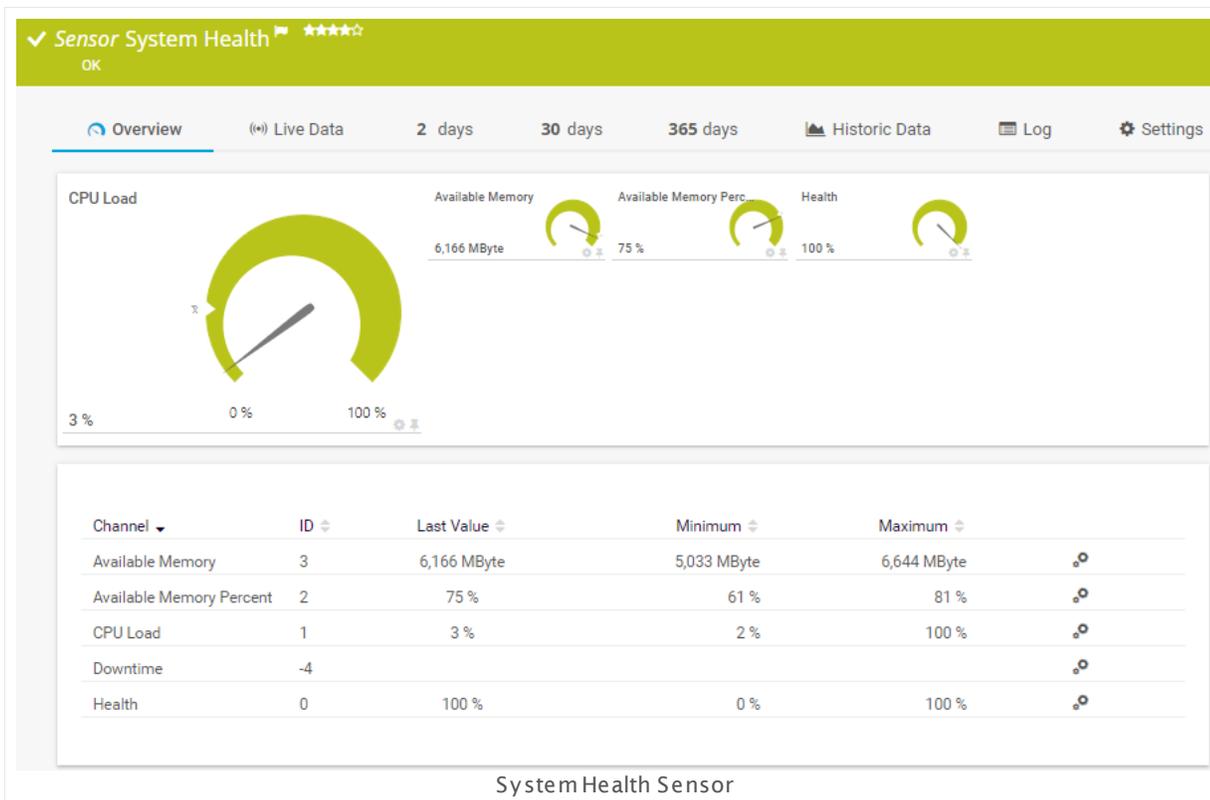
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.210 System Health Sensor

The System Health sensor monitors internal PRTG parameters. It shows the status of the system on which a probe runs. PRTG creates this sensor type automatically and cannot be deleted.

It checks various parameters of your PRTG system that can affect the quality of the monitoring results:

- **Health:** This index value sums up the probe state into a value between 100% (healthy) and 0% (failing). Frequent or repeated health values below 100% should be investigated.
- **Available Memory:** This channel shows the amount of free memory available on the system. This value should not fall below 500 MB. This way, PRTG can still request resources during report generation, auto-discoveries, and other issues.
- **Available Memory Percent:** This channel shows the free memory available on the system in percent.
- **System CPU Load:** This channel shows the current percentage CPU load on the system with the probe. Extensive CPU load can lead to false, incomplete, and incorrect monitoring results. This value should usually stay below 50%.



Sensor in Other Languages

Dutch: **System Status**, French: **État du système**, German: **Systemzustand**, Japanese: ? ? ? ? ? ? , Portuguese: **Funcionamento do sistema**, Russian: **Работоспособность системы**, Simplified Chinese: ? ? ? ? ? ? , Spanish: **Salud del sistema**

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR DISPLAY

Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-----------------	--

SENSOR DISPLAY

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁶⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

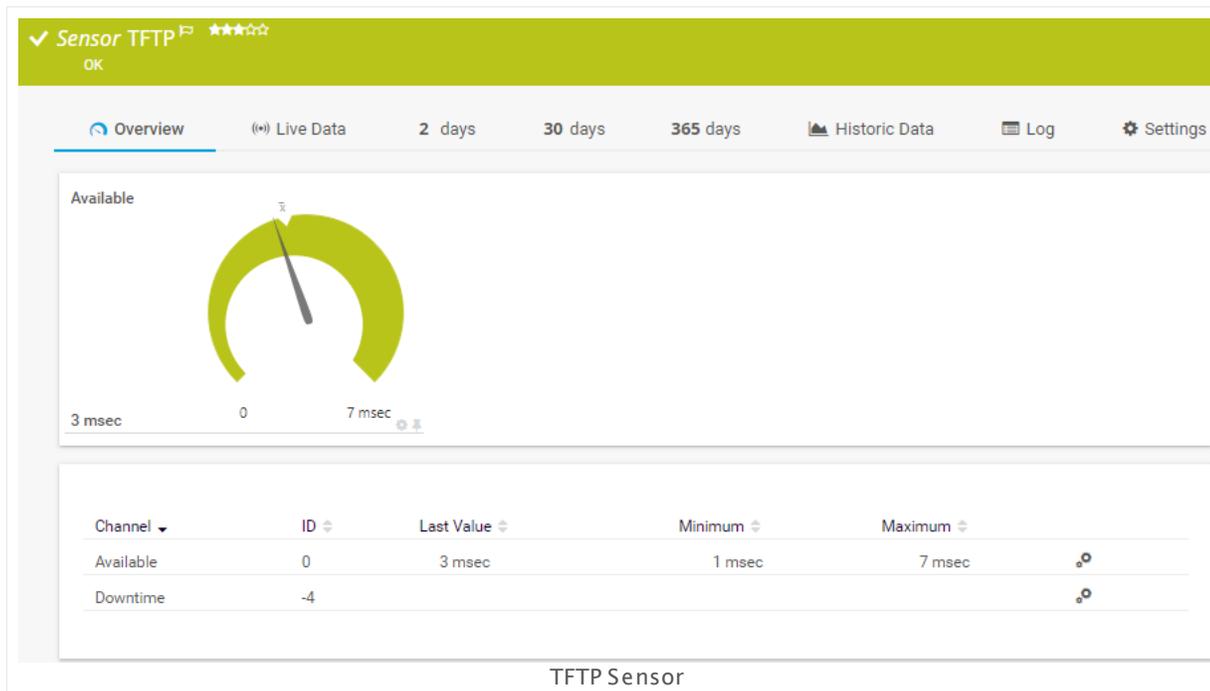
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.211 TFTP Sensor

The TFTP sensor monitors a Trivial File Transfer Protocol (TFTP) server and checks if a certain file is available for download.

- It shows the response time of the server.



Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).
Port	Enter the number of the port the TFTP service is running on. The sensor connects to this port. Please enter an integer value.
Filename	Enter the name of the file that this sensor checks. If this file name is not available on the server, the sensor shows a Down status ^[195] . Please enter a string.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p>i This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

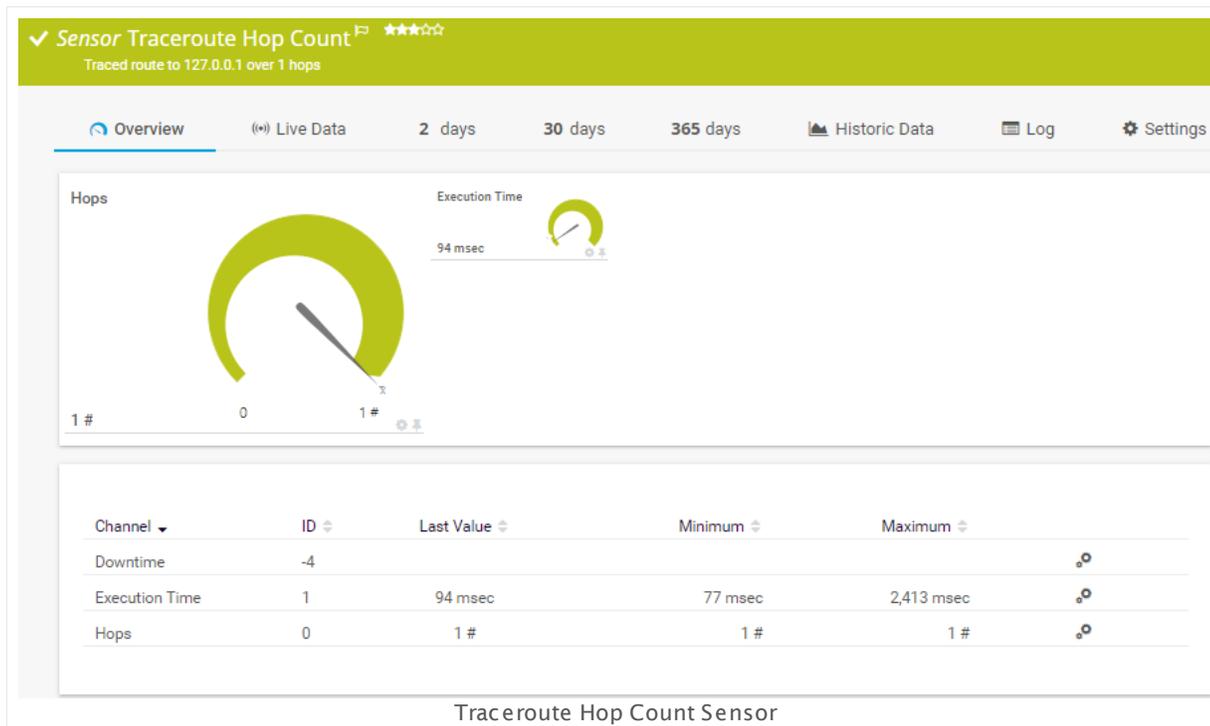
7.8.212 Traceroute Hop Count Sensor

The Traceroute Hop Count sensor traces the number of hops needed from the probe system the sensor is running on to the **IP Address/DNS Name** defined in the sensor's parent device.

It shows the following:

- Execution time
- Number of hops
- If the number of hops (the route) changes, you can additionally define another [sensor status](#)

195.



Sensor in Other Languages

Dutch: **Traceroute Hop Count**, French: **Traceroute Hop Count**, German: **Traceroute Hop Count**, Japanese: **Traceroute Hop Count**, Portuguese: **Rastreo de rotas**, Russian: **Трассировка маршрута**, Simplified Chinese: ? ? ? , Spanish: **Traceroute Hop Count**

Remarks

- [Requires](#) .NET 4.5 or later to be installed on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

If Route Changes Define what to do if the route has changed since the last check. Choose between:

- **Ignore**: Do not perform any action.
- **Set sensor to "Warning"**: The sensor will show a **Warning status**^[195] if the route has changed.
- **Set sensor to "Error"**: The sensor will show a **Down status**^[195] if the route has changed.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

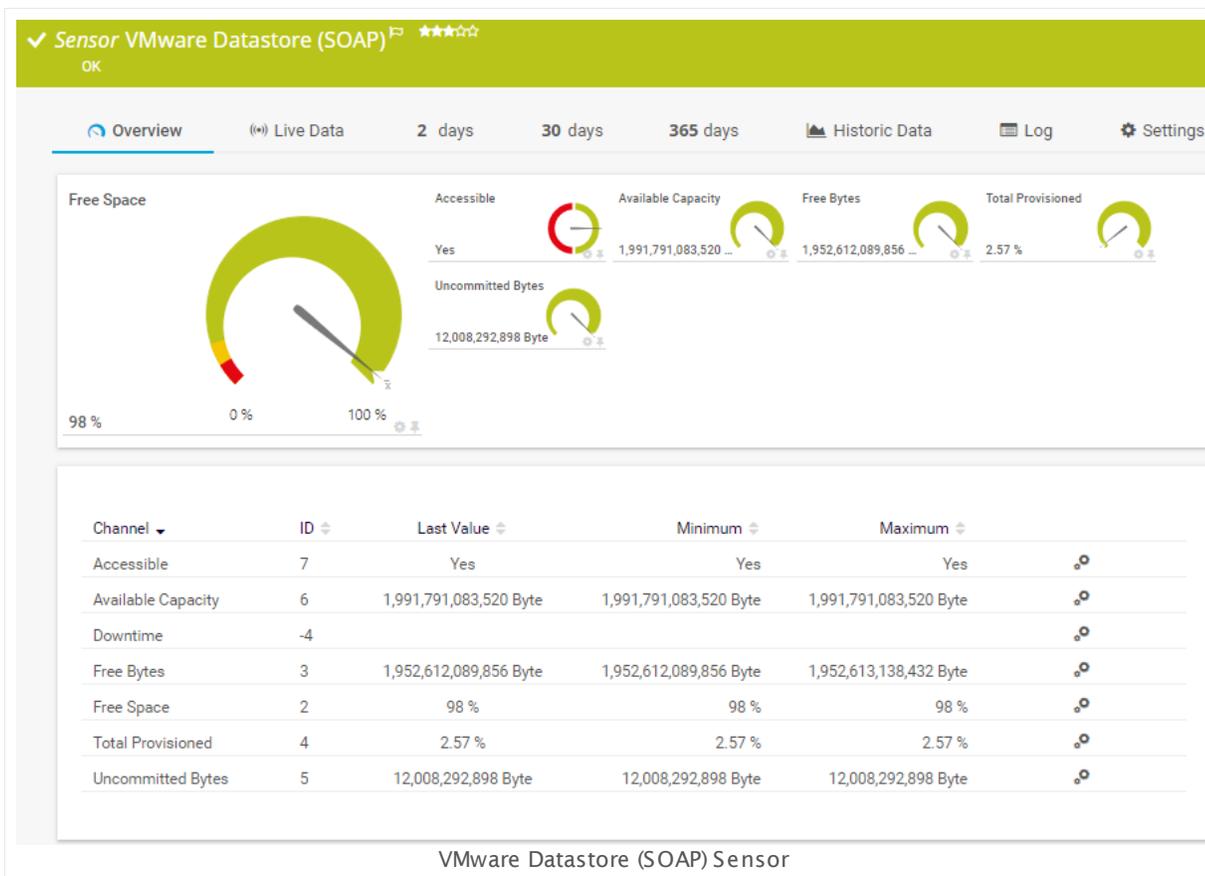
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.213 VMware Datastore (SOAP) Sensor

The VMware Datastore (SOAP) sensor monitors the disk usage of a VMware data store using Simple Object Access Protocol (SOAP). It can show the following:

- Available capacity in bytes: This is the physically or virtually available size of the data store.
- Free space in bytes and percent: This is the disk space that is not used by virtual machines. Used disk space can be either thick-provisioned or used from thin-provisioned virtual disks.
- Uncommitted bytes: This is the disk space that is provisioned for thin-provisioned virtual machines but not used yet.
- Total provisioned disk space in percent: This is the sum of all potentially used disk space of thin-provisioned and thick-provisioned VM hard drives (uncommitted bytes plus used bytes).
- Accessibility of the data store



Sensor in Other Languages

Dutch: **VMware Datastore (SOAP)**, French: **VMware Datastore (SOAP)**, German: **VMware Datastore (SOAP)**, Japanese: **VMware Datastore (SOAP)** , Portuguese: **VMware Datastore (SOAP)**, Russian: **Хранилище данных VMware (SOAP)**, Simplified Chinese: **VMware ? ? ? (SOAP)**, Spanish: **Almacén de datos VMware**

Remarks

- [Requires](#) ²⁶⁹³ .NET 4.5 or later to be installed on the probe system.
 - For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
 - The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, 6.0, or 6.5 or vCenter.
 - We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
 - Knowledge Base: [I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?](#)
 - Knowledge Base: [Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?](#)
 - This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#) ³⁶⁹³.
 - This sensor type has predefined limits for several metrics. You can change these limits individually in the channel settings. For detailed information about channel limits, refer to the manual section [Sensor Channels Settings](#) ³¹⁶⁰.
-  This sensor type supersedes the outdated SSH VMWare ESX(i) Disk sensor. We recommend that you use this new VMware Datastore (SOAP) sensor to monitor VMware data stores.

Requirement: .NET Framework

- ✘ This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

-  For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#) ³⁷⁰⁸ or when running a [cluster](#) ¹³⁰¹ setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

-  For details about this setting, see the Knowledge Base: [How can I increase the connection limit on VMware systems?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the data stores you want to monitor. PRTG will create one sensor for each data store you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

DATASTORE SETTINGS

Datastore Select all data stores for which you want to add a sensor. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

- Tags** Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.
- You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.
-  It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).
- Priority** Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DATASTORE SETTINGS

- MoID** Shows the Managed Object ID (MoID) of the data store that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result**: Do not store the sensor result.

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <https://kb.paessler.com/en/topic/30643>

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- <https://kb.paessler.com/en/topic/59173>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
213 VMware Datastore (SOAP) Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

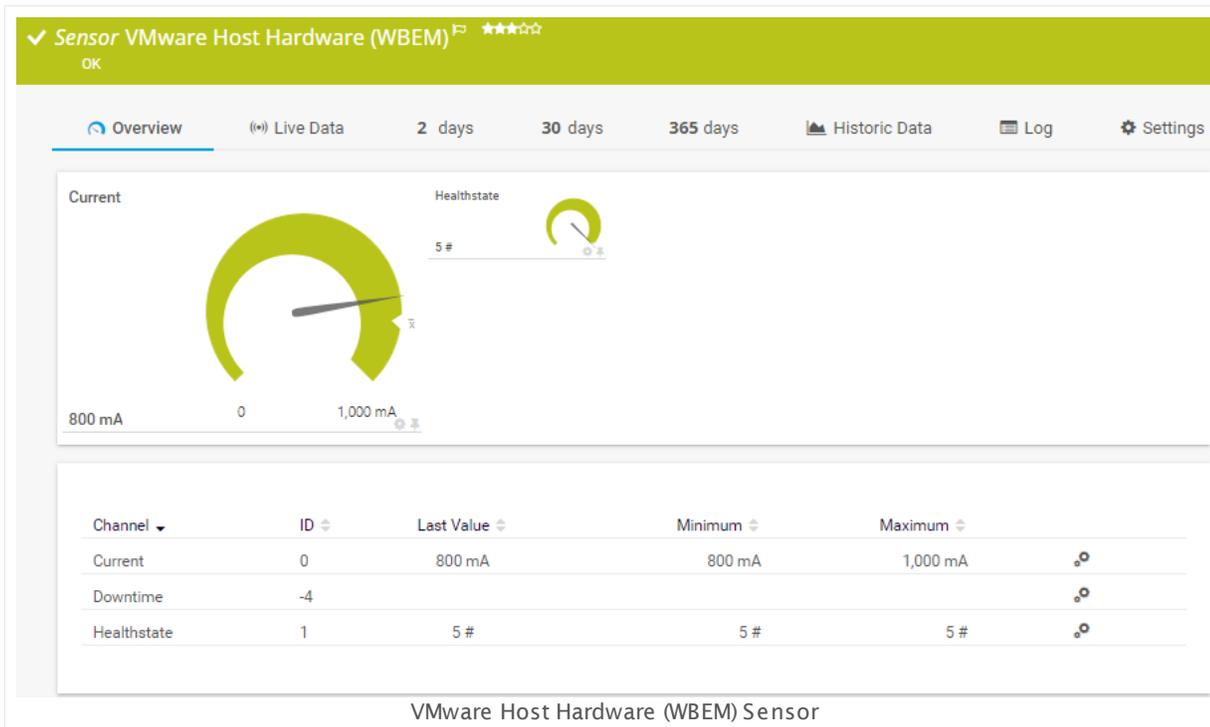
7.8.214 VMware Host Hardware (WBEM) Sensor

The VMware Host Hardware sensor monitors hardware information of an ESX/ESXi server using Web-Based Enterprise Management (WBEM).

It can show the following, depending on the selected ESX component:

- Health status
- Temperature
- Power
- Fan rotations per minute (RPM)
- Battery voltage

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **VMware Host Hardware (WBEM)**, French: **Matériel hôte VMware (WBEM)**, German: **VMware Host Hardware (WBEM)**, Japanese: **VMware? ? ? ? ? ? ? ? (WBEM)** , Portuguese: **VMware Hardware do host (WBEM)**, Russian: **Аппаратные средства узла VMware (WBEM)**, Simplified Chinese: **VMware? ? ? ? (WBEM)**, Spanish: **Hardware de host VMware (WBEM)**

Remarks

- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, 6.0, or 6.5.
- For this sensor type you must define credentials for Linux/Solaris/Mac OS (SSH/WBEM) systems on the device you want to use the sensor on.
- [Requires](#) ²⁷⁰⁴ the CIM interface to be enabled on the ESXi host. On ESXi 6.5 and later you have to manually enable CIM.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: Enabled CIM Interface on ESXi Host

To access the ESXi host and retrieve monitoring data via WBEM, the Common Information Model (CIM) interface must be enabled on the ESXi host. On ESXi 6.5, CIM is disabled by default so you have to activate it manually.

 For details, see this Knowledge Base article: [How do I enable the CIM interface on VMware ESXi 6.5?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the ESXi components you want to monitor. PRTG will create one sensor for each hardware element you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

ESXI SERVER ELEMENTS

ESXi Element	Select the hardware elements you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
--------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

ESX SERVER ELEMENTS

Element	Shows the ESX element that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Automatic Sensor State	<p>Define if the sensor will change its status¹⁹⁵ dependent on the health state reading. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor state automatically to 'Warning' or 'Down': Set the sensor to a Warning or Down status when the server returns respective values. The sensor will additionally change to a Down status if the connection to the server fails. ▪ Just report the current reading, ignore Server Health Value: Never change the sensor's status dependent on the values returned by the server. The sensor will only change to a Down status if the connection to the server fails.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How do I enable the CIM interface on VMware ESXi 6.5?

- <https://kb.paessler.com/en/topic/76255>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
214 VMware Host Hardware (WBEM) Sensor

Others

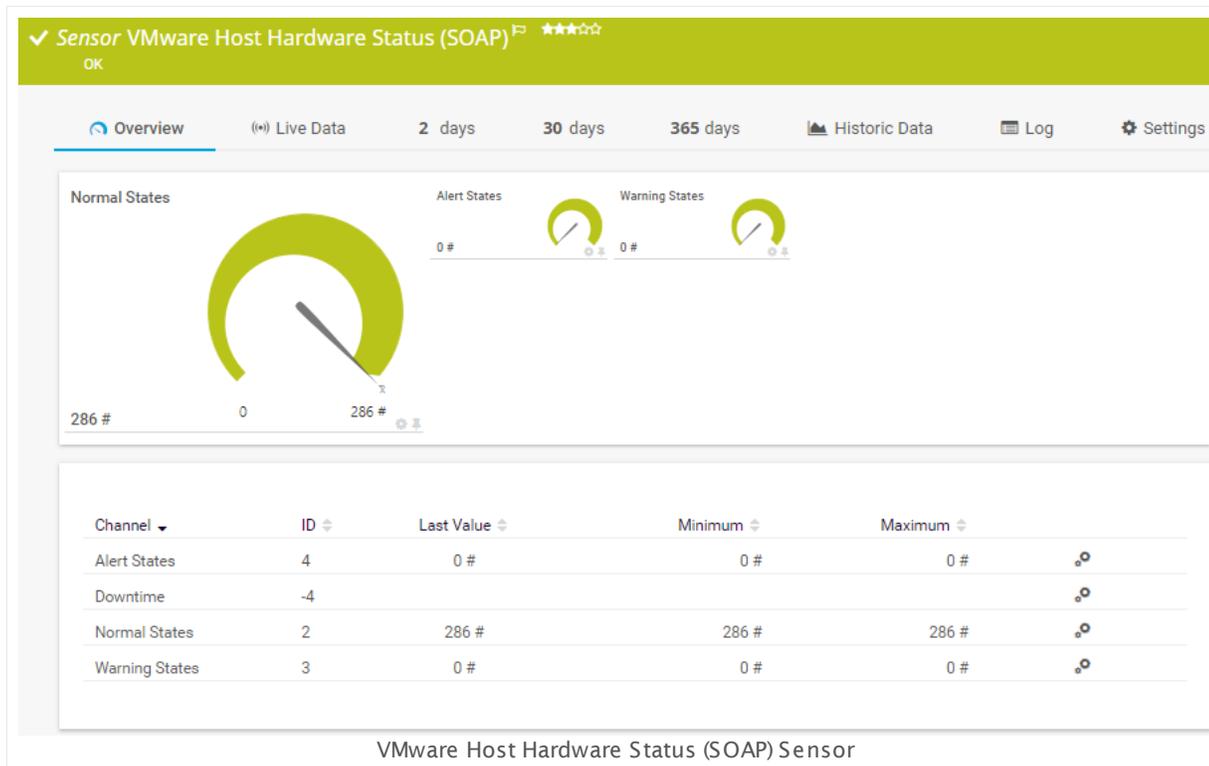
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.215 VMware Host Hardware Status (SOAP) Sensor

The VMware Host Hardware Status (SOAP) sensor monitors the hardware status of a VMware host server using Simple Object Access Protocol (SOAP).

- It shows the total number of items in **normal**, **warning**, and **alert** status, just as the vSphere client reports.

This sensor is intended to give you a general status overview for your host. Any states other than "normal" will be reported in the sensor message.



Sensor in Other Languages

Dutch: **VMware Host Hardware Status (SOAP)**, French: **État du matériel du serveur hôte VMware (SOAP)**, German: **VMware Hostserver Hardware-Zustand (SOAP)**, Japanese: **VMware ? ? ? ? ? ? ? ? ? (SOAP)** , Portuguese: **VMware Status do hardware de host (SOAP)**, Russian: **Состояние аппаратных средств узла VMware (SOAP)**, Simplified Chinese: **VMware ? ? ? ? ? ? (SOAP)**, Spanish: **Estado de hardware de VMware Host (SOAP)**

Remarks

- [Requires](#) ²⁷¹⁴ .NET 4.5 or later to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).

- This sensor only shows items that report an actual status, so you might see more "sensors" in your vSphere client than the number of states available in the channels of this PRTG sensor.
- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, 6.0, or 6.5. We recommend that you do not use this sensor type on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?](#)
- Knowledge Base: [Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[3706] or when running a [cluster](#)^[130] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For details about this setting, see the Knowledge Base: [How can I increase the connection limit on VMware systems?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the VMware hosts you want to monitor. PRTG will create one sensor for each host server you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VMWARE HOST SETTINGS

Host Server Select the host server you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)^[181], as well as in [alarms](#)^[213], [logs](#)^[228], [notifications](#)^[3216], [reports](#)^[3262], [maps](#)^[3278], [libraries](#)^[3235], and [tickets](#)^[230].

Parent Tags Shows [Tags](#)^[139] that this sensor [inherits](#)^[140] from its [parent device, group, and probe](#)^[133]. This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#)^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)^[140] from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE HOST SETTINGS

MoID Shows the Managed Object ID (MoID) of the host that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Known Warnings Enter one or more semicolon (;) separated warning messages from the VMware host that you want to ignore. Messages that you enter here will not affect the [sensor status](#)^[195]. Please enter a string or leave the field empty.

i We strongly recommend that you use this filter for known issues only. For example, various systems (mainly HP and IBM systems) return unknown states because of errors in the the vendors' CIM extensions. Because of this, you might not get an [Up status](#)^[195] for this sensor at all although your vSphere client does not show warnings. In this case, use this filter option and enter the known warning message(s), for example, **Power Supply 7;Power Supply 8**

Known Errors Enter one or more semicolon (;) separated error messages from the VMware host that you want to ignore. Messages that you enter here will not affect the [sensor status](#)^[195]. Please enter a string or leave the field empty.

i We strongly recommend that you use this filter for known issues only. For example, various systems (mainly HP and IBM systems) return unknown states because of errors in the the vendors' CIM extensions. Because of this, you might not get an [Up status](#)^[195] for this sensor at all although your vSphere client does not show errors. In this case, use this filter option and enter the known error message(s), for example, **Power Supply 7;Power Supply 8**

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <https://kb.paessler.com/en/topic/30643>

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
215 VMware Host Hardware Status (SOAP) Sensor

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- <https://kb.paessler.com/en/topic/59173>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.216 VMware Host Performance (SOAP) Sensor

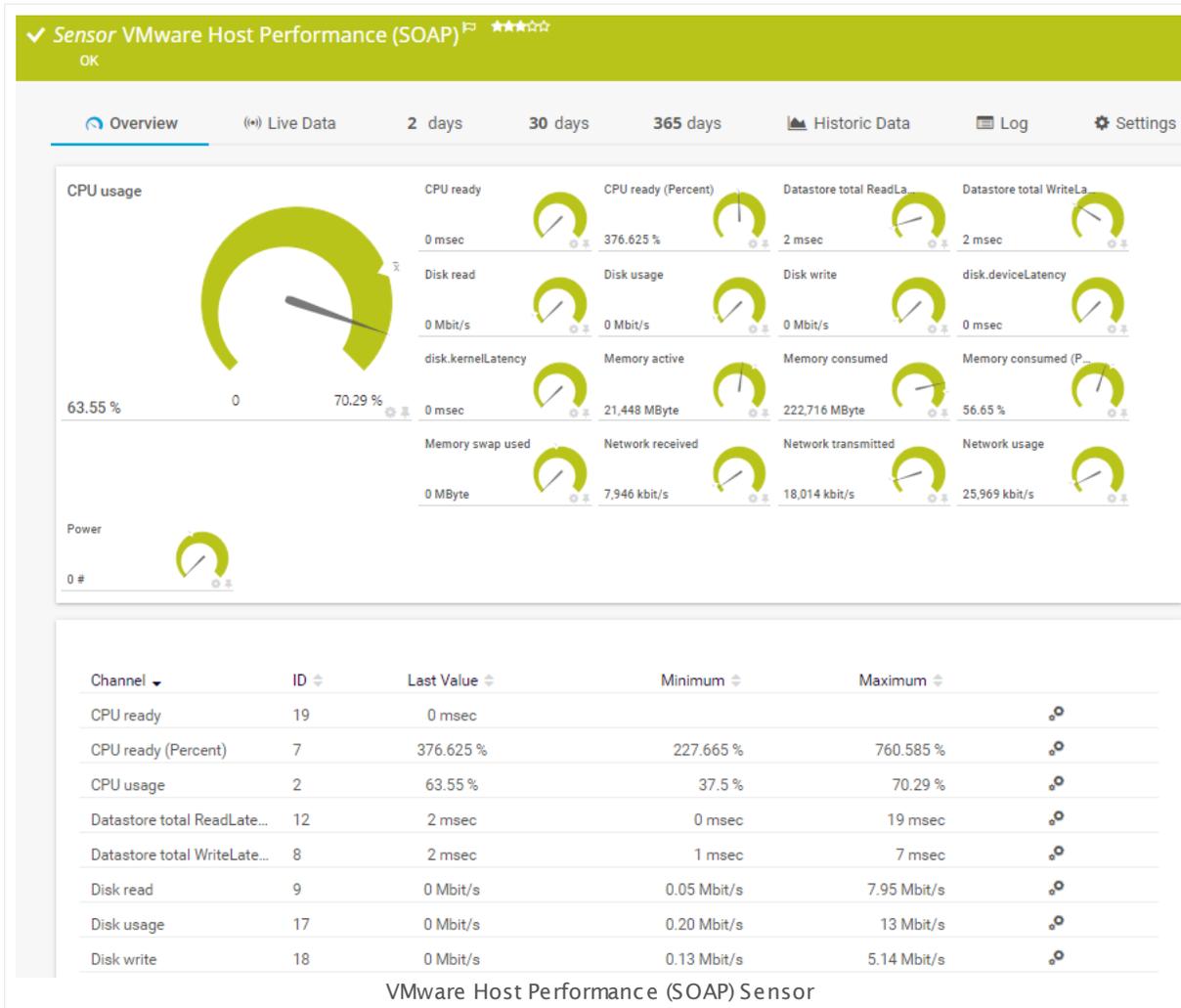
The VMware Host Performance (SOAP) sensor monitors a VMware host server using Simple Object Access Protocol (SOAP).

It can show the following:

- CPU usage in percent
- CPU ready in percent
- Network usage
- Disk usage
- Disk read and write speed
- Active memory in bytes
- Consumed memory in bytes and percent
- Used memory swap
- Disk and data store latency (read and write)
- Network received and transmitted speed
- Power status

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 216 VMware Host Performance (SOAP) Sensor



Sensor in Other Languages

Dutch: **VMware Host Prestaties (SOAP)**, French: **Performances de l'hôte VMware (SOAP)**, German: **VMware Host server Leistung (SOAP)**, Japanese: **VMware ? ? ? ? ? ? ? ? ? ? (SOAP)**, Portuguese: **VMware Performance do host (SOAP)**, Russian: **Работа узла VMware (SOAP)**, Simplified Chinese: **VMware ? ? ? ? (SOAP)**, Spanish: **Rendimiento de VMware Host (SOAP)**

Remarks

- [Requires](#) .NET 4.5 or later to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
- The parent device must be a VMware ESXi server version 5.0, 5.1, 5.5, 6.0, or 6.5. We recommend that you do not use this sensor type on your vCenter. Reliable hardware information can only be provided when this sensor is created on your physical host server as parent device.

- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?](#)
- Knowledge Base: [Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[3709] or when running a [cluster](#)^[130] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For details about this setting, see the Knowledge Base: [How can I increase the connection limit on VMware systems?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE HOST SETTINGS

MoID	Shows the Managed Object ID (MoID) of the host that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
------	--

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between:
---------------	---

DEBUG OPTIONS

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <https://kb.paessler.com/en/topic/30643>

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
216 VMware Host Performance (SOAP) Sensor

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- <https://kb.paessler.com/en/topic/59173>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.217 VMware Virtual Machine (SOAP) Sensor

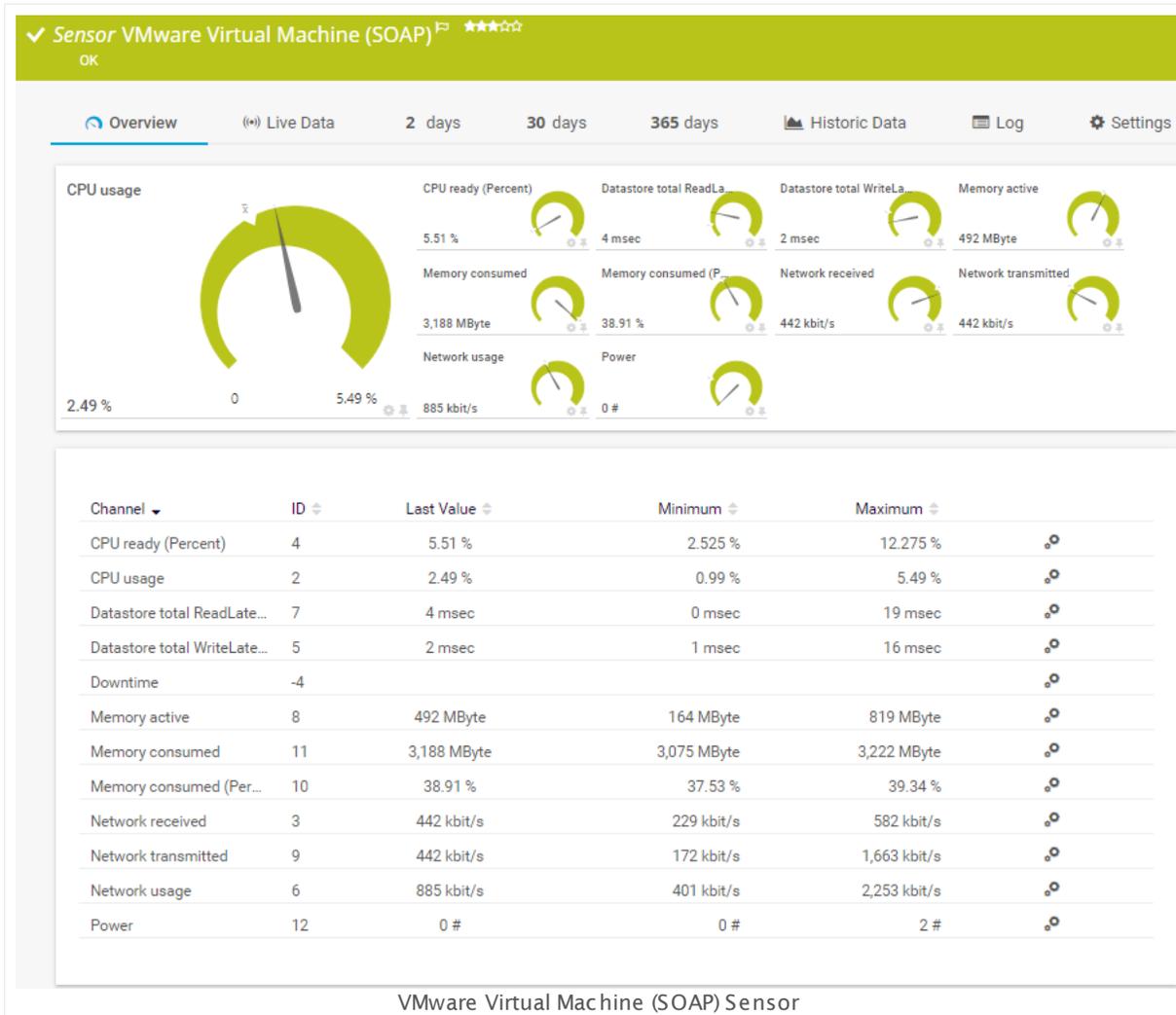
The VMware Virtual Machine (SOAP) sensor monitors a virtual machine on a VMware host server using Simple Object Access Protocol (SOAP).

It shows the following:

- CPU usage in percent
- CPU ready in percent
- Active memory in bytes
- Consumed memory in bytes and percent
- Disk read and write speed
- Read and write latency
- Network usage (total, received, and transmitted bytes per second)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 217 VMware Virtual Machine (SOAP) Sensor



VMware Virtual Machine (SOAP) Sensor

Sensor in Other Languages

Dutch: **VMware Virtuele Machine (SOAP)**, French: **Machine virtuelle VMware (SOAP)**, German: **VMware Virtual Machine (SOAP)**, Japanese: **VMware? ? ? ? ? (SOAP)** , Portuguese: **VMware Máquina virtual (SOAP)**, Russian: **Виртуальная машина VMware (SOAP)**, Simplified Chinese: **VMware? ? ? (SOAP)**, Spanish: **Máquina virtual VMware (SOAP)**

Remarks

- [Requires](#) .NET 4.5 or later to be installed on the probe system.
- For this sensor type you must define credentials for VMware servers on the device you want to use the sensor on. Ensure you enter a user with sufficient access rights to obtain statistics (read-only usually works).
- We recommend that you use **vCenter** as parent device. When the monitored VM changes the host server via **vMotion**, PRTG can continue monitoring in this case. The sensor can monitor VMware ESXi server version 5.0, 5.1, 5.5, 6.0, or 6.5.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.

- For VMware virtual machines, disk usage channels are only available as of virtual hardware version 8.
- Knowledge Base: [I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?](#)
- Knowledge Base: [Why are my VMware sensors not working after upgrading to VCSA 6.5 U1?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Settings on VMware Host System

If you set up this sensor on different probes (for example, when using [remote probes](#)^[3708] or when running a [cluster](#)^[130] setup), you might need to change the settings of your VMware host, so it accepts more incoming connections. Otherwise you might get connection timeouts when running plenty of VMware sensors with a short scanning interval.

 For details about this setting, see the Knowledge Base: [How can I increase the connection limit on VMware systems?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

 PRTG requests a full list of all virtual machines configured on the device. Because of this, it may take a few seconds before the dialog is loaded.

Select the VMware virtual machines you want to monitor. PRTG will create one sensor for each virtual machine you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VIRTUAL MACHINE SETTINGS

Virtual Machine You see a list of all virtual machines (VMs) available on the host server on this device, including the ones that are not running. All VMs are listed by name and the OS they are running on.

Select the desired items by adding check marks in front of the respective lines. One sensor will be created for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

VMWARE VIRTUAL MACHINE SETTINGS

MoID Shows the Managed Object ID (MoID) of the virtual machine that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Handling of "Powered Off" VM Define the sensor behavior for a virtual machine that is powered off. Choose between:

- **Ignore "powered off" state (default):** The sensor will not change to a **Down status** ¹⁹⁵ if the virtual machine is powered off. It will report zero values instead.
- **Alarm when VM is "powered off":** The sensor will change to a **Down status** ¹⁹⁵ if the virtual machine is powered off.
 While in Down status, a sensor does not record any data in any of its channels.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#) ³⁷³⁴.

DEBUG OPTIONS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration ³³⁵ on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none"> ▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request. ▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error. ▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests. ▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests. ▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests. ▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. <p> Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.</p> <p> If a sensor has defined error limits for channels, it will always show a Down status immediately, so no "wait" option will apply.</p> <p> If a channel uses lookup³⁶⁹³ values, it will always show a Down status immediately, so no "wait" options will apply.</p> |

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How can I increase the connection limit on VMware systems?

- <https://kb.paessler.com/en/topic/30643>

Knowledge Base: Monitoring ESXi 5.1 and higher: Handshake Failure on Windows XP/Server 2003

- <https://kb.paessler.com/en/topic/59173>

Knowledge Base: For which sensor types do you recommend Windows Server 2012 R2 and why?

- <https://kb.paessler.com/en/topic/64331>

Knowledge Base: I cannot add VMware sensors because of "wrong" password although it is correct. What can I do?

- <https://kb.paessler.com/en/topic/66794>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

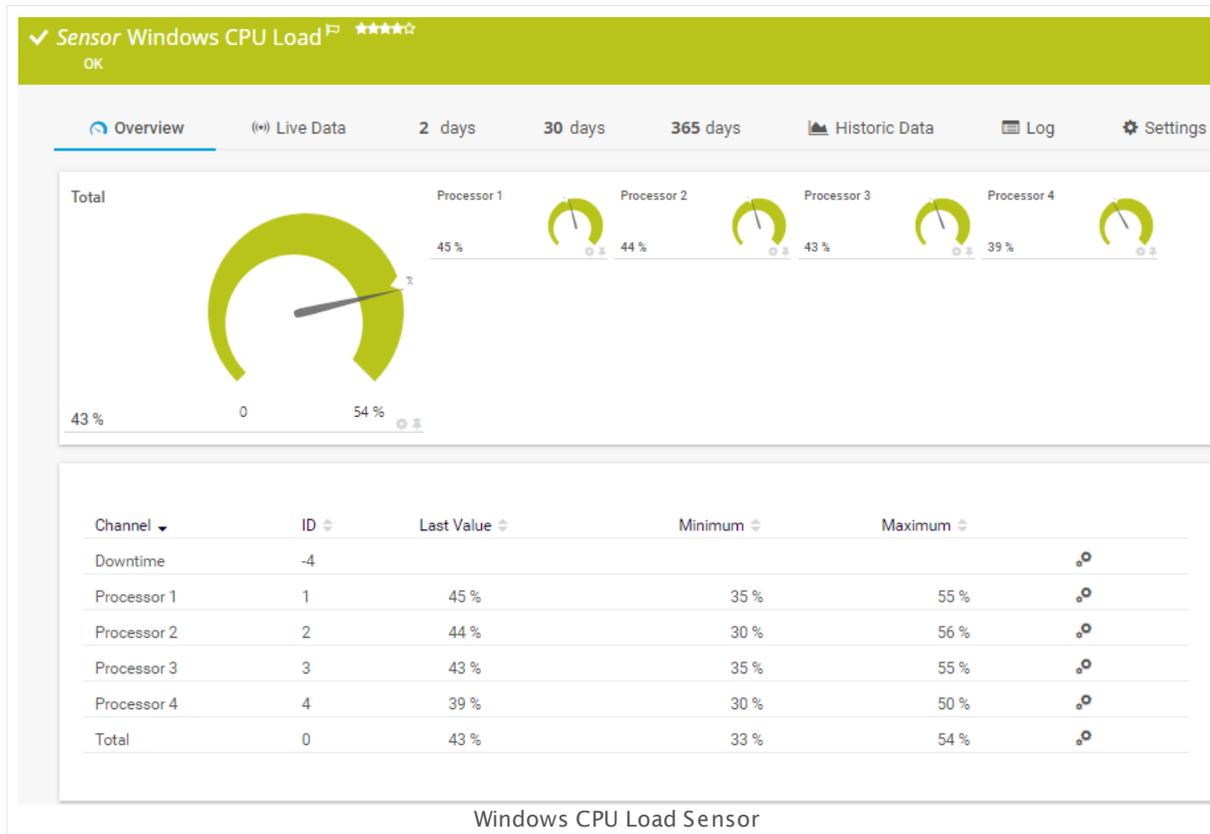
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.218 Windows CPU Load Sensor

The Windows CPU Load sensor monitors the CPU load on a computer via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the CPU usage of all processors and the total load in percent.



Sensor in Other Languages

Dutch: **Windows Processor Belasting**, French: **Charge CPU de Windows**, German: **Windows Prozessorlast**, Japanese: **Windows CPU ? ?**, Portuguese: **Windows Carga de CPU**, Russian: **Загрузка ЦП Windows**, Simplified Chinese: **Windows CPU ? ?**, Spanish: **WMI carga de procesador**

Remarks

- [Requires](#) ²⁷⁴⁵ Windows credentials in the [parent device settings](#) ⁴⁰².
- [Requires](#) ²⁷⁴⁵ Windows 2008 R2 or later on the probe system.
- [Requires](#) ²⁷⁴⁶ the Windows Remote Registry service to be running on the target computer.
- [Requires](#) ²⁷⁴⁵ WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.

- [Can use a hybrid approach](#)^[2745] to query monitoring data: Performance counters as standard approach and WMI as fallback.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[3709].

 WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value. You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags .

BASIC SENSOR SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

WMI ALTERNATIVE QUERY

Errors and Invalid Data This is an extended help field only. WMI sensors in PRTG are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do so in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like **class not valid** or **invalid data**.

Wherever possible, PRTG features an alternative query that might work in your specific configuration. If you keep getting errors for this sensor, please try enabling the alternative query method below.

WMI ALTERNATIVE QUERY

- Alternative Query Choose the method PRTG uses to query via WMI. For compatibility reasons, you can enable an alternative query method. We recommend that you use the default value. You can choose between:
- **Use default (recommended):** Use the PRTG standard method to query WMI. This is the best setting in most cases.
 - **Use alternative (if default does not work):** Use an alternative method to query WMI. If you keep getting errors with the default setting, try this setting.

SENSOR DISPLAY

- Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
-  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#) settings).
- Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.219 Windows IIS 6.0 SMTP Received Sensor

The Windows IIS 6.0 SMTP Received sensor monitors the number of received emails for a Microsoft Internet Information Services (IIS) 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the number and bytes of received messages.

Sensor in Other Languages

Dutch: **WMI IIS 6.0 SMTP Ontvangen**, French: **Windows IIS 6.0 SMTP reçu**, German: **WMI IIS 6.0 SMTP Empfangen**, Japanese: **Windows IIS 6.0 SMTP** ? ? , Portuguese: **Windows IIS 6.0 SMTP recebido**, Russian: **Получено пакетов Windows IIS 6.0 SMTP**, Simplified Chinese: ? ? ?
Windows IIS 6.0 SMTP, Spanish: **WMI IIS 6.0 SMTP Recibidos**

Remarks

- [Requires](#) ^[2754] Windows credentials in the [parent device settings](#) ^[402].
- [Requires](#) ^[2755] Windows 2008 R2 or later on the probe system.
- [Requires](#) ^[2755] the Windows Remote Registry service to be running on the target computer.
- [Requires](#) ^[2755] WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
- [Can use a hybrid approach](#) ^[2755] to query monitoring data: Performance counters as standard approach and WMI as fallback.
- This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

i By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

A Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.

i For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[357] section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[370].

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between:
---------------	---

DEBUG OPTIONS

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.220 Windows IIS 6.0 SMTP Sent Sensor

The Windows IIS 6.0 SMTP Sent sensor monitors the number of sent emails for a Microsoft Internet Information Services (IIS) 6.0 SMTP service (Exchange 2003) using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It shows the following:

- Number and bytes of sent messages
- Number of retries per second for sent messages

Sensor in Other Languages

Dutch: **WMI IIS 6.0 SMTP Verzonden**, French: **Windows IIS 6.0 SMTP envoyé**, German: **WMI IIS 6.0 SMTP Verschickt**, Japanese: **Windows IIS 6.0 SMTP** ? ? , Portuguese: **Windows IIS 6.0 SMTP enviado**, Russian: **Отправлено пакетов Windows IIS 6.0 SMTP**, Simplified Chinese: ? ? ?
Windows IIS 6.0 SMTP, Spanish: **WMI IIS 6.0 SMTP Enviados**

Remarks

- [Requires](#) ^[2763] Windows credentials in the [parent device settings](#) ^[402].
- [Requires](#) ^[2764] Windows 2008 R2 or later on the probe system.
- [Requires](#) ^[2764] the Windows Remote Registry service to be running on the target computer.
- [Requires](#) ^[2764] WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
- [Can use a hybrid approach](#) ^[2764] to query monitoring data: Performance counters as standard approach and WMI as fallback.
- This service is not used by Exchange Server 2007 and higher. Exchange Server 2007 uses its own SMTP stack implemented in the Microsoft Exchange Transport service.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

i By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

A Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.

i For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[357] section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[370].

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between:
---------------	---

DEBUG OPTIONS

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

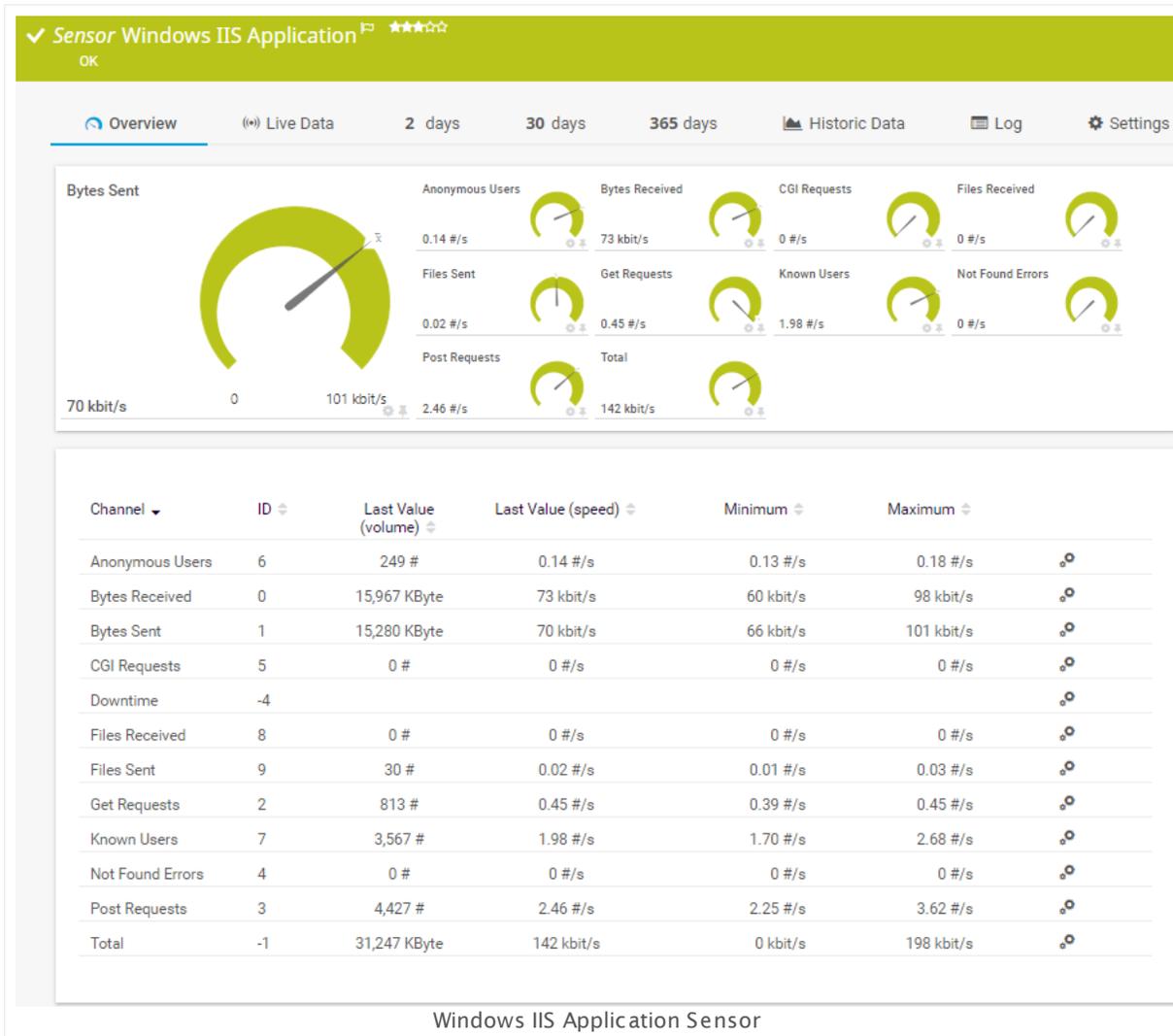
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.221 Windows IIS Application Sensor

The Windows IIS Application sensor monitors a Microsoft Internet Information Services (IIS) server via Windows Management Instrumentation (WMI). It can also monitor applications that use IIS, such as Microsoft SharePoint or Microsoft Reporting Services (SSRS).

It shows the following:

- Sent and received bytes per second
- Number of sent and received files per second
- Number of anonymous and known users per second
- Number of Common Gateway Interface (CGI) requests per second
- Number of GET and POST requests per second
- Number of not found errors per second



Windows IIS Application Sensor

Sensor in Other Languages

Dutch: **Windows IIS Toepassing**, French: **Application Windows IIS**, German: **Windows IIS-Anwendung**, Japanese: **Windows IIS** ? ? ? ? ? ? ? ? , Portuguese: **Windows Aplicação IIS**, Russian: **Приложение Windows IIS**, Simplified Chinese: **Windows IIS** ? ? ? ? , Spanish: **Aplicación IIS WMI**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)¹²⁵. Above this number, please consider using multiple [Remote Probes](#)³⁷⁰⁹ for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)³⁵⁰⁷.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the web service instances you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI INTERNET INFORMATION SERVICES

Specify Instance	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
------------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI INTERNET INFORMATION SERVICES

Instance Shows the name of the web service instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

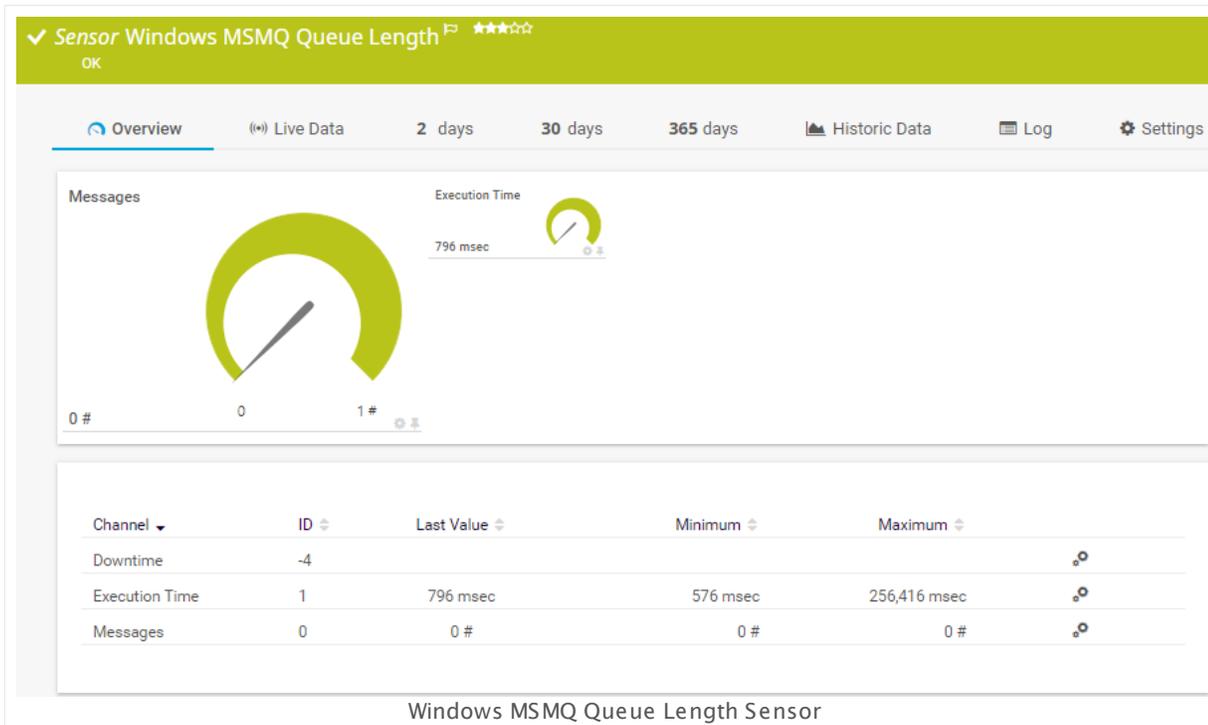
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.222 Windows MSMQ Queue Length Sensor

The Windows MSMQ Queue Length sensor reads the number of messages in a Microsoft Message Queue of the parent device.

It shows the following:

- Total number of messages in the queue
- Execution time



Sensor in Other Languages

Dutch: **Windows MSMQ wachtrijlengte**, French: **Longueur de la file d'attente MSMQ de Windows**, German: **Windows MSMQ Queue-Länge**, Japanese: **Windows MSMQ ? ? ? ? ?**, Portuguese: **Windows Comprimento da fila MSMQ**, Russian: **Длина очереди Windows MSMQ**, Simplified Chinese: **Windows MSMQ ? ? ? ?**, Spanish: **Largo de queue de Windows MSMQ**

Remarks

- [Requires](#)^[2783] .NET 4.5 or later to be installed on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- [Requires](#)^[2783] Windows credentials in the [parent device settings](#)^[402].
- [Requires](#)^[2783] the MSMQ service to be running on both the probe and the target system.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [How do I activate Message Queuing in my Windows installation?](#)

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: Message Queuing Service

In order for this sensor to work, the **MSMQ** "Message Queuing" service must be started both on the target system and on the computer running the PRTG probe: Either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. Additionally, the MSMQ "Message Queuing" service must also be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Depending on your Windows version you may first need to install the **Microsoft Message Queue (MSMQ) Server**.

 When installing Microsoft Message Queue (MSMQ) Server, make sure you install it including the **Directory Service**. Depending on your Windows installation this might have a different name, such as:

- MSMQ Active Directory Domain Service Integration
- Directory Service Integration

- Active Directory Integration

 For details, see the Knowledge Base: [How do I activate Message Queuing in my Windows installation?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the message queues you want to monitor. PRTG will create one sensor for each queue you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Message Queue

You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. If there are no message queues available, you will see a corresponding message.

 This sensor cannot monitor sub-queues.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Message Queue	Shows the name of the queue that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Message Queue Type	Shows the type of the queue that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Min. Message Age	Optionally define an age in minutes the message has to be old to be counted. If set, messages younger than this age are not regarded. If you leave this field blank, the sensor will not check for the message age. Please enter an integer value or leave the field empty.

SENSOR SETTINGS

If Value Changes

Define what this sensor will do when the sensor value changes. You can choose between:

- **Ignore changes (default):** The sensor takes no action on change.
- **Trigger 'change' notification:** The sensor sends an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#) ³⁷⁷⁰ whenever the sensor value changes.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#) ³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: How do I activate Message Queuing in my Windows installation?

- <https://kb.paessler.com/en/topic/25963>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
222 Windows MSMQ Queue Length Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.223 Windows Network Card Sensor

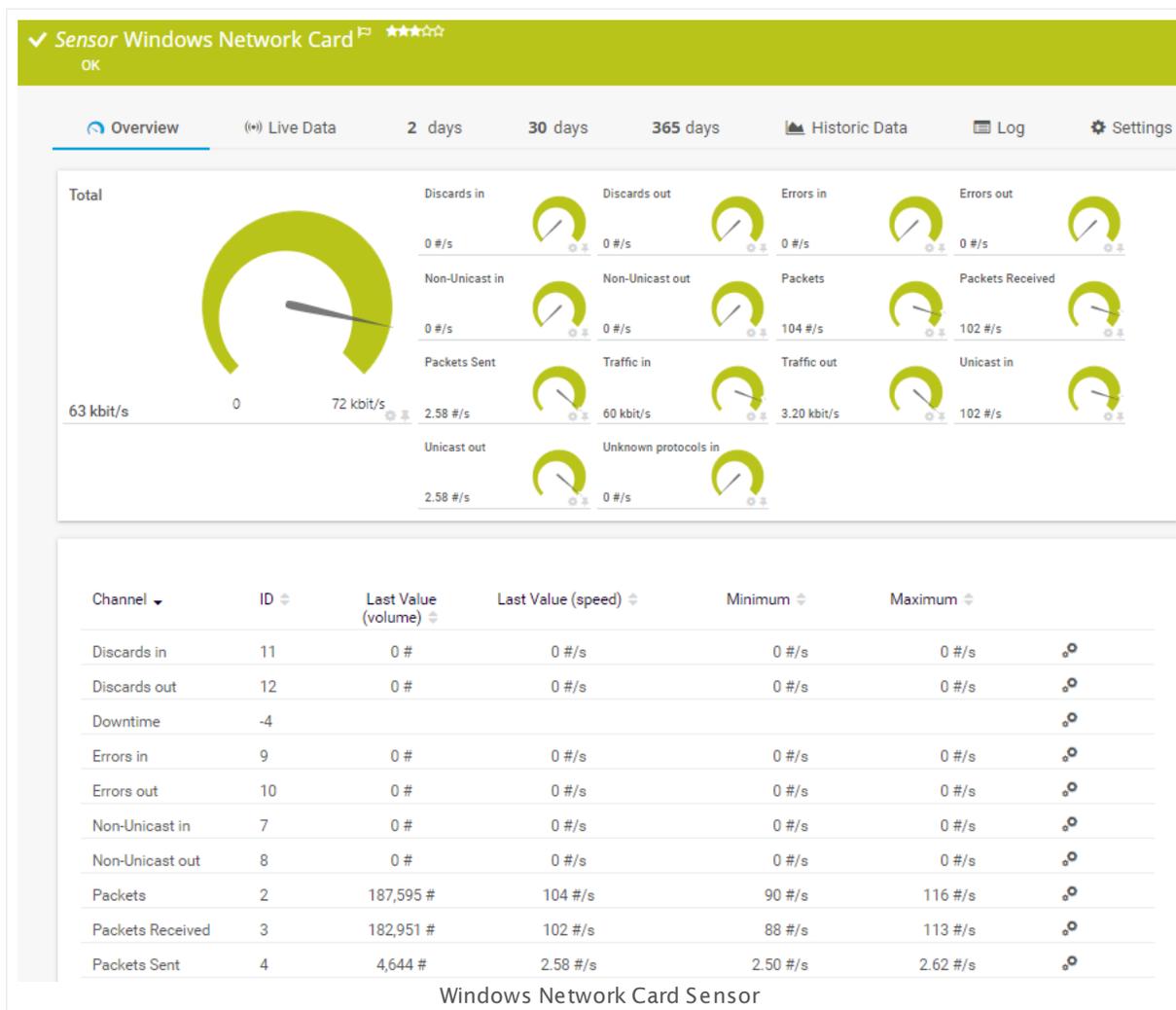
The Windows Network Card sensor monitors bandwidth usage and traffic of a network interface using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It can show the following:

- Total traffic on the network card
- Traffic in and traffic out
- Number of received and sent packets
- Total number of packets
- Number of discards (in and out)
- Number of errors (in and out)
- Number of unicast packets (in and out)
- Number of non-unicast packets (in and out)
- Number of unknown protocols (in)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
 223 Windows Network Card Sensor



Sensor in Other Languages

Dutch: **Windows Netwerkaart**, French: **Carte réseau Windows**, German: **WMI Netzwerkadapter**, Japanese: **Windows ? ? ? ? ? ? ? ? ?**, Portuguese: **Windows Adaptador de rede**, Russian: **Сетевой адаптер Windows**, Simplified Chinese: **Windows ? ?**, Spanish: **WMI tarjeta de red**

Remarks

- [Requires](#) ^[2795] Windows credentials in the [parent device settings](#) ^[402].
- [Requires](#) ^[2795] Windows 2008 R2 or later on the probe system to work with Windows Performance Counters.
- [Requires](#) ^[2795] the Windows Remote Registry service to be running on the target computer.
- [Requires](#) ^[2795] WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.

- [Can use a hybrid approach](#)^[2795] to query monitoring data: Performance counters as standard approach and WMI as fallback.
- Requires Windows Server 2008 R2 or Windows 7 or later to be able to monitor 64-bit counters of the class **Network Adapter** (virtual network interfaces). On older target systems the sensor can only monitor 32-bit counters of the class **Network Interface** (the physical interface) and will show less channels.
- This sensor type supports teamed network adapters ("NIC teaming") on Windows Server 2012.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[3708].

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

x In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the network cards you want to monitor. PRTG will create one sensor for each interface you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SPECIFIC

Network Interface	Select the network card(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
-------------------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Selected Interface	Shows the name of the network card that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
--------------------	--

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed underneath the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking on the pin symbol of a channel in the sensor's overview tab.

Chart Type

Define how to show different channels for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.

SENSOR DISPLAY

- **Show in and out traffic as positive and negative area chart:** Show channels for incoming and outgoing traffic as positive and negative area chart. This will visualize your traffic in a clear way.

 You cannot use this option in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰). Manual scaling is not possible if you choose this option.

 You cannot show a positive/negative chart for a channel if you choose to display its data in percent of maximum (available in the [Sensor Channels Settings](#)³¹⁶⁰).

Stack Unit

This setting is only available if you choose **Stack channels on top of each other** above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking, if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

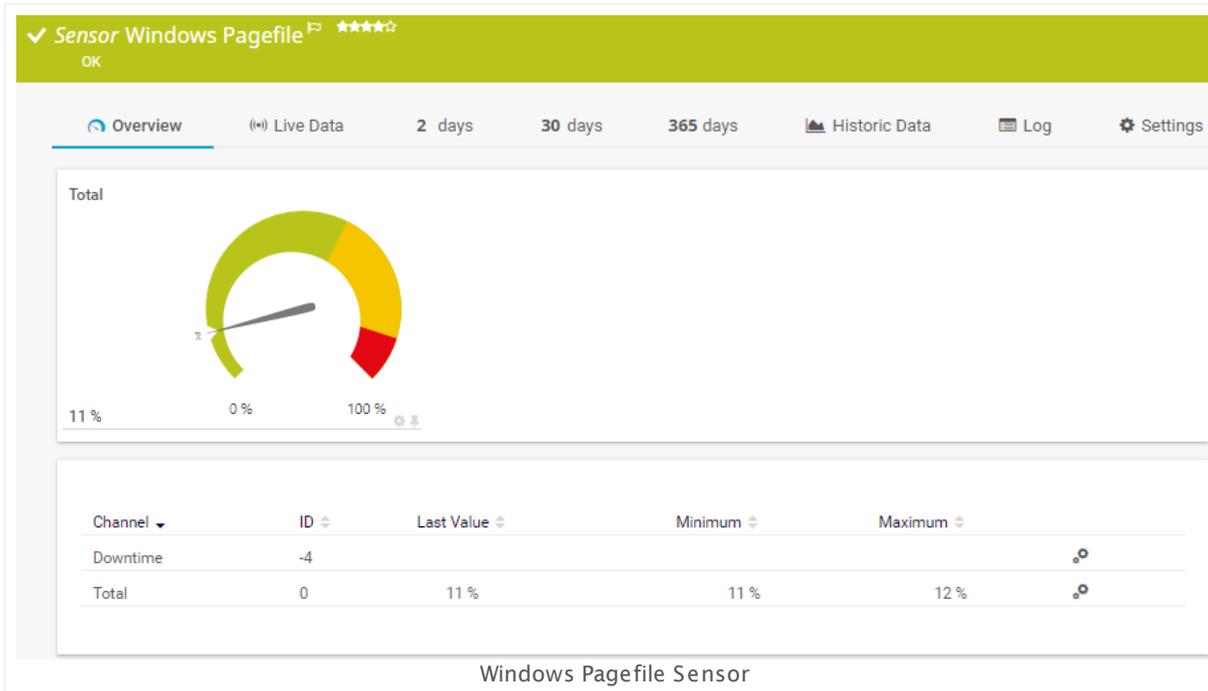
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.224 Windows Pagefile Sensor

The Windows Pagefile sensor monitors the Windows pagefile usage via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the pagefile usage in percent.



Sensor in Other Languages

Dutch: **Windows Wisselbestand**, French: **Fichier d'échange Windows**, German: **WMI Auslagerungsdatei**, Japanese: **Windows** ? ? ? ? ? ? ? , Portuguese: **Windows Arquivo de Paginação (Pagefile)**, Russian: **Файл подкачки Windows**, Simplified Chinese: **Windows** ? ? ? ? ? , Spanish: **Archivo de página Windows**

Remarks

- This sensor does not work with Windows 2000, because the respective WMI class does not exist on this operating system!
- [Requires](#) Windows credentials in the [parent device settings](#).
- [Requires](#) Windows 2008 R2 or later on the probe system.
- [Requires](#) the Windows Remote Registry service to be running on the target computer.
- [Requires](#) WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
- [Can use a hybrid approach](#) to query monitoring data: Performance counters as standard approach and WMI as fallback.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[3705].

 WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

 In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📖 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

- User Group Access
- Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:
- **Inherited:** Use the access rights settings of the parent object.
 - **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
 - **Read:** Users in this group can see the object and review its monitoring results.
 - **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
 - **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
224 Windows Pagefile Sensor

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.225 Windows Physical Disk I/O Sensor

The Windows Physical Disk I/O sensor monitors the input/output parameters of a hard disk on a Windows system via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

The sensor provides the following information:

- Disk Latency
- Disk Bandwidth
- Disk queue data
- Disk IOs

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

✓ Sensor Windows Physical Disk I/O ^P ★★☆☆☆

OK

Overview | Live Data | 2 days | 30 days | 365 days | Historic Data | Log | Settings

Disk Read Time %

<1 % 0 % 100 %

Avg Bytes Per Read	881,711 #	Avg Bytes Per Transfer	46,089 #	Avg Bytes Per Write	9,786 #	Avg Queue	< 0.01 #
Avg Read Queue	< 0.01 #	Avg Read Time	0 msec	Avg Transfer Time	0 msec	Avg Write Queue	< 0.01 #
Avg Write Time	0 msec	Current Queue	0 #	Disk IOs	1.47 #/s	Disk Read	0.43 Mbit/s
Disk Read IOs	0.06 #/s	Disk Time %	<1 %	Disk Transfer	0.54 Mbit/s	Disk Write	0.11 Mbit/s
Disk Write IOs	1.41 #/s	Disk Write Time %	<1 %	Idle Time %	>99 %	Split IOs	0.04 #/s

Channel	ID	Last Value	Minimum	Maximum	
Avg Bytes Per Read	4	881,711 #	0 #	5,266,074 #	🔊
Avg Bytes Per Transfer	5	46,089 #	5,073 #	102,712 #	🔊
Avg Bytes Per Write	6	9,786 #	4,880 #	102,743 #	🔊
Avg Queue	8	< 0.01 #	0 #	0.02 #	🔊
Avg Read Queue	7	< 0.01 #	< 0.01 #	0.03 #	🔊
Avg Read Time	10	0 msec	0 msec	0 msec	🔊
Avg Transfer Time	11	0 msec	0 msec	0 msec	🔊
Avg Write Queue	9	< 0.01 #	0 #	0.02 #	🔊
Avg Write Time	12	0 msec	0 msec	0 msec	🔊

Windows Physical Disk I/O Sensor

Sensor in Other Languages

Dutch: **Windows Fysieke Schijf I/O**, French: **E/S du disque physique de Windows**, German: **Windows Physikalischer Datenträger E/A**, Japanese: **Windows I/O**, Portuguese: **Windows E/S do Disco físico**, Russian: **Ввод-вывод физического диска Windows**, Simplified Chinese: **Windows I/O**, Spanish: **Operaciones de E/S de disco físico Windows**

Remarks

- **Requires** Windows credentials in the [parent device settings](#).
- **Requires** Windows 2008 R2 or later on the probe system.
- **Requires** the Windows Remote Registry service to be running on the target computer.
- **Requires** WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
- **Can use a hybrid approach** to query monitoring data: Performance counters as standard approach and WMI as fallback.
- Currently, this sensor type is in beta status. The methods of operating can change at any time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's Credentials for Windows Systems](#) settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

 In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#)^[3705].

 WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

 In order for this sensor to work with Windows Performance Counters, please make sure the [Remote Registry](#) Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the physical disk(s) you want to monitor. PRTG will create one sensor for each disk you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WINDOWS PHYSICAL DISK SPECIFIC

Physical Disk(s) Select the disk(s) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS PHYSICAL DISK SPECIFIC

Physical Disk(s) Shows the disk this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)^[3734].
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

❗ The result of this sensor is only written to disk if you use **WMI only (recommended)** as **Preferred Data Source**, as defined in the [Windows Compatibility Options](#)^[415] of the parent device.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

- ❗ You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.226 Windows Print Queue Sensor

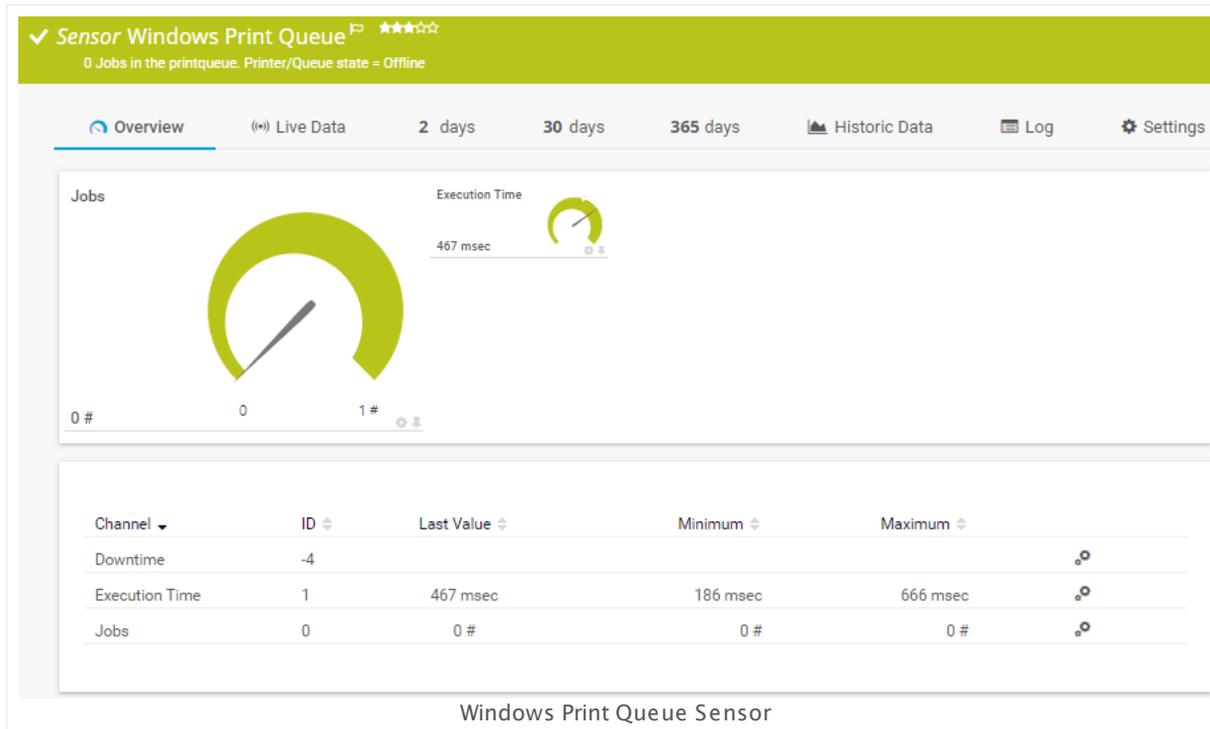
The Windows Print Queue sensor reads the print queue on its parent device and returns the number of jobs in the print queue. It can monitor queues for all printers that are installed locally.

For example, you can use this sensor to monitor all print queues on your Windows print server and retrieve information about all available jobs that are in the queue longer than defined.

It shows the following:

- Number of jobs in the queue
- Execution time

Additionally, this sensor can change to a defined status if there is a printer problem. See section [Sensor Settings](#)²⁸²⁶ for available parameters.



Sensor in Other Languages

Dutch: **Windows Print Queue**, French: **File d'attente d'impression Windows**, German: **Windows Druckwarteschlange**, Japanese: **Windows ? ? ? ? ? ? ?**, Portuguese: **Windows Fila de impressão**, Russian: **Очередь печати Windows**, Simplified Chinese: **Windows ? ? ? ?**, Spanish: **Queue de impresión Windows**

Remarks

- [Requires](#)²⁸²⁷ .NET 4.5 or later to be installed on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.

- [Requires](#) ²⁸²⁷ Windows credentials in the [parent device settings](#) ⁴⁰².
 - [Requires](#) ²⁸²⁷ the Print Spooler Windows service to be running on the target device.
 - We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
 - You can add a ['change' trigger](#) ³³¹⁶ to this sensor to get a notification when the number of jobs in the queue changes.
 - This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) ⁴⁰⁷ **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: Print Spooler Service

In order for this sensor to work, the **Spooler** "Print Spooler" service must be started on the target computer.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the print queues you want to monitor. PRTG will create one sensor for each task you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SENSOR SETTINGS

Print Queue

You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. If there are no print queues available, you will see a corresponding message.

 If a printer name changes after you have created a sensor for its queue, please add the sensor anew.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name

Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#)¹⁸¹, as well as in [alarms](#)²¹⁹, [logs](#)²²⁸, [notifications](#)³²¹⁶, [reports](#)³²⁵², [maps](#)³²⁷⁶, [libraries](#)³²³⁵, and [tickets](#)²³⁰.

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

Print Queue	Shows the name of the task that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Advanced Status Option	<p>You can optionally define specific sensor states for several return messages of the monitored printer. Choose between:</p> <ul style="list-style-type: none">▪ Hide: Do not define sensor states for specific return messages.▪ Show: If you choose this option, you can define sensor states for various messages that the monitored printer reports.
Door Open	<p>These settings are only available if you select the advanced status option above. For each reported problem of the monitored printer, you can define the status that the sensor will show. Choose between:</p> <ul style="list-style-type: none">▪ Ignore: The current sensor status will persist if this message is reported by the printer.

SENSOR SETTINGS

Manual Feed Required	▪ Warning: The sensor will show a Warning status if this message is reported by the printer.
Needs User Intervention	▪ Error: The sensor will show a Down status if this message is reported by the printer.
Offline	
Out of Memory	
Out of Paper	
Paper Jammed	
Paper Problem	
Paused	
Printer Error	
Printer Not Available	
Toner Low	
Toner Out	
Min. Print Job Age (Sec.)	Optionally define the age of the print job in seconds. If set, jobs younger than this value are not regarded. If you leave this field empty, the sensor will not check for the print job age. Please enter an integer value or leave the field empty.

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between: <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	---

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.227 Windows Process Sensor

The Windows Process sensor monitors a Windows process using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

It shows the following parameters about the process:

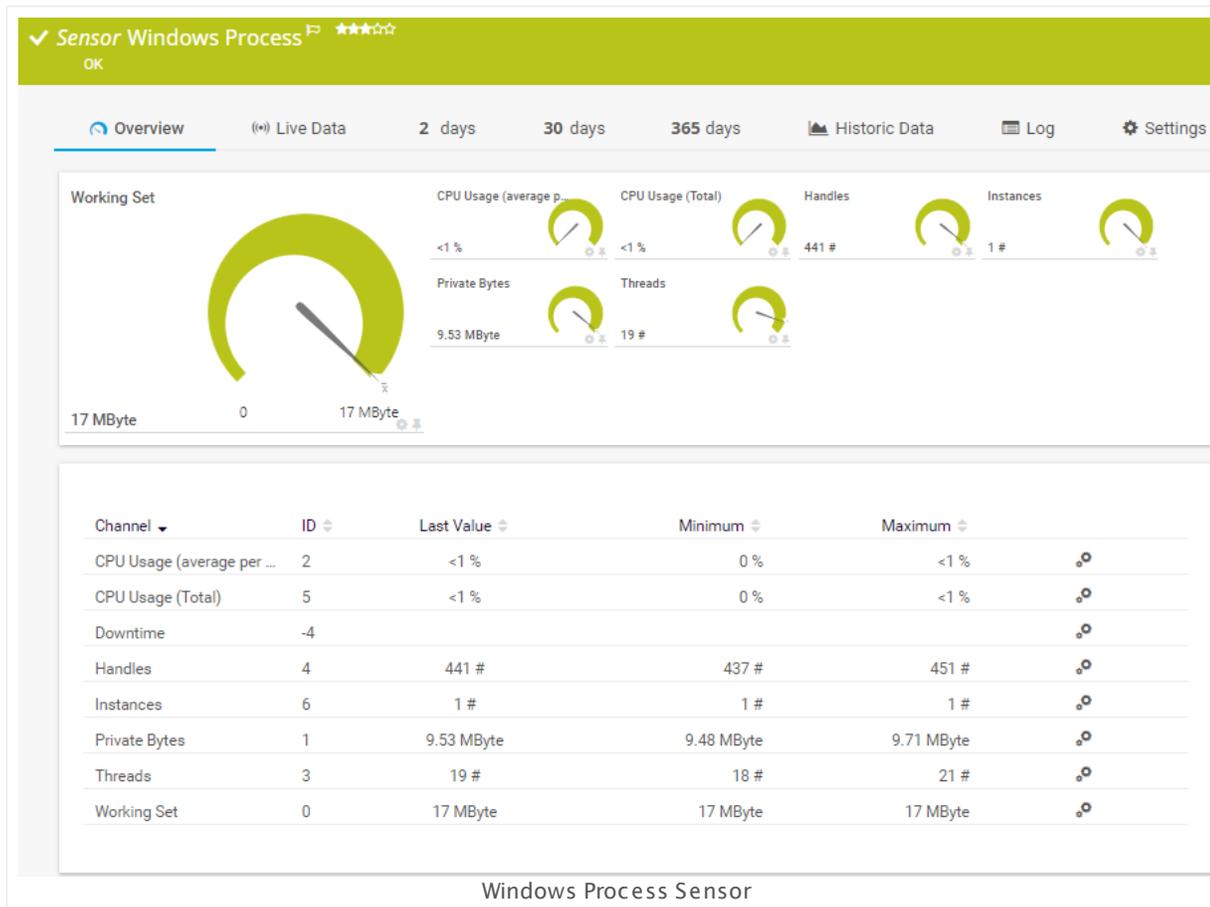
- Absolute working set in bytes
- Private bytes
- Number of threads
- Number of handles
- Number of instances
- Average CPU usage (if there are multiple instances running)
- Total CPU usage

i For the **CPU Usage (Total)** value of a process, all CPU usage values are summed up. The total is divided by the number of all CPUs and the maximum value is 100%. This corresponds to the CPU usage of all instances of this specific process.

i For the **CPU Usage (average per instance)** value, the summed up CPU usage value is divided by the number of all instances. It shows the average CPU usage of a single instance of the process on one CPU.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

227 Windows Process Sensor



Sensor in Other Languages

Dutch: **Windows Proces**, French: **Processus Windows**, German: **Windows Prozess**, Japanese: **Windows ? ? ? ?**, Portuguese: **Windows Processo**, Russian: **Процесс Windows**, Simplified Chinese: **Windows ? ?**, Spanish: **Proceso de Windows**

Remarks

- [Requires](#) ^[2838] Windows credentials in the [parent device settings](#) ^[402].
- [Requires](#) ^[2840] Windows 2008 R2 or later on the probe system.
- [Requires](#) ^[2840] the Windows Remote Registry service to be running on the target computer.
- [Does not support 64-bit processes](#) ^[2839] on devices with the address **localhost**, **127.0.0.1**, **::1**. Use the IP address in the network instead.
- The sensor cannot show values above 4 GB for 64-bit processes if you run the probe on a 64-bit Windows system. Please add this sensor to a probe running on a 32-bit Windows to monitor 64-bit processes.
- [Requires](#) ^[2840] WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.

- [Can use a hybrid approach](#)^[2839] to query monitoring data: Performance counters as standard approach and WMI as fallback.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Monitoring 64-bit Processes

This sensor type does not support 64-bit processes on devices with the address **localhost**, **127.0.0.1** (IPv4 address), or **::1** (IPv6 address) in PRTG. This is the case for probe devices, for example. The sensor works on all other target devices in your network. So if you want to monitor 64-bit processes on your local machine, [add this device](#)^[311] to PRTG with one of the IP addresses under which it is reachable in the local network (for example, 10.0.10.20 instead of 127.0.0.1) and create the sensor on this device.

 This sensor type cannot show values above 4 GB for 64-bit processes if you run the PRTG probe with this sensor on a 64-bit Windows system. The **WoW64 (Windows 32-bit on Windows 64-bit)** emulation layer for 32-bit applications like PRTG limits monitoring values from 64-bit systems or processes to 4 GB and caps off greater values. To avoid this issue that is caused by Windows and to correctly monitor 64-bit processes, please add this sensor to a probe that runs on a 32-bit Windows system.

Requirement: Windows Credentials

 Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

 By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#)^[415] on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

 Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

 For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#)^[3507] section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#).

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

BASIC SENSOR SETTINGS

Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WINDOWS PROCESS MONITOR

Executable	<p>Enter the name of the process that you want to monitor. Provide the name of an executable file without the <code>.exe</code> extension (for example, enter <code>firefox</code> to monitor <code>firefox.exe</code>).</p> <p> The sensor will show a Down status if the process is not active on the device.</p>
------------	---

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.
---------------	--

DEBUG OPTIONS

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

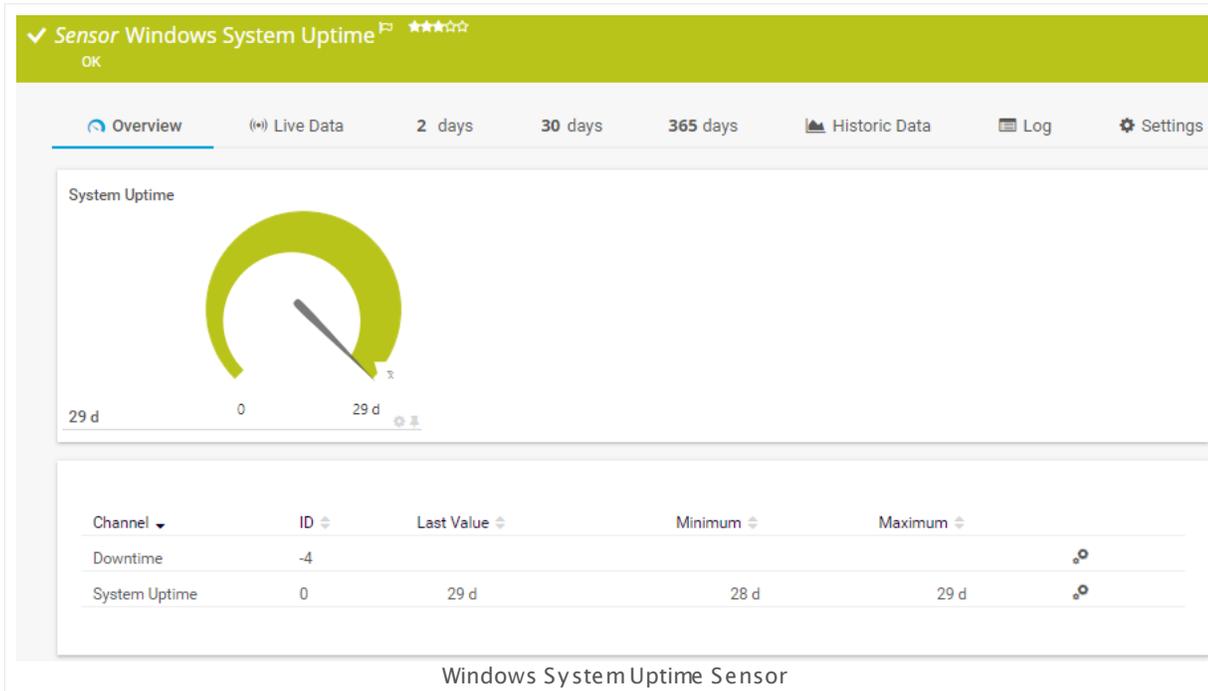
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.228 Windows System Uptime Sensor

The Windows System Uptime sensor monitors the uptime of a Windows system using Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device.

- It shows the total uptime of the system in days, hours, minutes.



Sensor in Other Languages

Dutch: **Windows System Uptime**, French: **Disponibilité du système Windows**, German: **Windows Systemlaufzeit**, Japanese: **Windows ? ? ? ? ? ? ? ?**, Portuguese: **Windows Tempo de ativação do sistema**, Russian: **Время бесперебойной работы системы Windows**, Simplified Chinese: **Windows ? ? ? ? ? ? ? ?**, Spanish: **Tiempo disponible Windows**

Remarks

- Requires** Windows credentials in the [parent device settings](#).
- Requires** Windows 2008 R2 or later on the probe system.
- Requires** the Windows Remote Registry service to be running on the target computer.
- Requires** WoW64 (Windows 32-bit on Windows 64-bit) for target systems that run Windows Server 2016.
- Can use a hybrid approach** to query monitoring data: Performance counters as standard approach and WMI as fallback.

You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: Windows Credentials

X Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#) [Credentials for Windows Systems](#) settings, please prefer using Windows domain credentials.

A If you use local credentials, please make sure the same Windows user accounts (with same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise, a connection via Performance Counters will not be possible. However, WMI connections may still work.

Hybrid Approach: Performance Counters and WMI

i By default, this sensor type uses Windows Management Instrumentation (WMI) to request monitoring data. You can change the default behavior to a **hybrid approach** in the **Windows Compatibility Options** of the parent [device's settings](#) on which you create this sensor: if you choose this option, the sensor will first try to query data via **Windows Performance Counters** and use WMI as a fallback if Performance Counters are not available. When running in fallback mode, the sensor will re-try to connect via Performance Counters after 24 hours.

A Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#). Above this number, please consider using multiple [Remote Probes](#) for load balancing.

i For a general introduction to the technology behind WMI, please see [Monitoring via WMI](#) section.

Requirement: Windows Version

X In order for this sensor to work with Windows Performance Counters, please make sure a Windows version 2008 or later is installed on the computer running the PRTG probe: This is either on the local system (on every node, if on a cluster probe), or on the system running a [remote probe](#).

i WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

Requirement: Remote Registry Service

X In order for this sensor to work with Windows Performance Counters, please make sure the **Remote Registry** Windows service is running on the target computer. If you fail to do so, a connection via Performance Counters will not be possible. However, WMI connections may still work.

To enable the service, please log in to the respective computer and open the services manager (for example, via [services.msc](#)). In the list, find the respective service and set its **Start Type** to **Automatic**.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My Windows sensors do not work when using direct Performance Counter access. What can I do?

- <https://kb.paessler.com/en/topic/47263>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.229 Windows Updates Status (Powershell) Sensor

The Windows Updates Status (PowerShell) sensor monitors the status of Windows updates on a computer and counts the available and installed Windows updates—either from Microsoft or from the local Windows Server Update Services (WSUS) server.

It can show the following:

- Elapsed time since the last update
- Installed Windows updates
- Missing Windows updates
- Hidden updates
- All updates are listed with their severity.

You can find the considered updates in [Server Manager \(WSUS\)](#) under **Roles | Windows Server Update Services | Update Services | Computers | Reports**.

✓ Sensor Windows Updates Status (Powershell) ★★★★☆

Ok

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Security Updates (Critical) Missing

0 #

Security Updates (Critical) 16 #

16 #

Security Updates (Important) 57 #

57 #

Security Updates (Important) 0 #

0 #

Security Updates (Low) 0 #

0 #

Security Updates (Low) 0 #

0 #

Security Updates (Moderate) 2 #

2 #

Security Updates (Moderate) 0 #

0 #

Time since last update 19 d

19 d

Updates (Severity Critical) 0 #

0 #

Updates (Severity Important) 0 #

0 #

Updates (Severity Low) 0 #

0 #

Updates (Severity Moderate) 0 #

0 #

Updates (Unclassified) 0 #

0 #

Windows Updates Installed 16 #

16 #

Windows Updates Missing 2 #

2 #

Channel	ID	Last Value	Minimum	Maximum	
Downtime	-4				
Security Updates (Critical) Missing	9	16 #	16 #	16 #	
Security Updates (Critical)	10	0 #	0 #	0 #	
Security Updates (Important)	7	57 #	57 #	57 #	
Security Updates (Important)	8	0 #	0 #	0 #	
Security Updates (Low)	3	0 #	0 #	0 #	
Security Updates (Low)	4	0 #	0 #	0 #	
Security Updates (Moderate)	5	2 #	2 #	2 #	
Security Updates (Moderate)	6	0 #	0 #	0 #	

Windows Updates Status (Powershell) Sensor

8/14/2018

2857

Sensor in Other Languages

Dutch: **Windows Updates Status (PowerShell)**, French: **Statut de mises à jour Windows (PowerShell)**, German: **Windows Updates Status (PowerShell)**, Japanese: **Windows ? ? ? ? ? ? ? ? ? ? (PowerShell)**, Portuguese: **Windows Status de atualizações (PowerShell)**, Russian: **Статус обновления Windows (PowerShell)**, Simplified Chinese: **Windows ? ? ? ? ? ? ? ? ? ? (PowerShell)**, Spanish: **Estados de actualizaciones de Windows (PowerShell)**

Remarks

- [Requires](#) ²⁸⁵⁸ .NET 4.5 or higher to be installed on the probe system.
 - [Requires](#) ²⁸⁵⁹ Remote PowerShell to be enabled on the target system and PowerShell 3.0 on both the probe system and the target system.
 - Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - The minimum scanning interval for this sensor is **1 hour**. It also might take some time to receive data for the first time after starting the sensor.
 - Knowledge Base: [PowerShell Sensors: FAQ](#)
 - If the sensor cannot determine the "Time since last update" (for example, because the list of updates is empty), it will show the value **-1s** and turn into a **Warning status** ¹⁹⁵.
 - We recommend that you set the [scanning interval](#) ²⁸⁶¹ of this sensor to at least 12 hours to limit the load on the server being monitored.
 - In certain cases, it might take some time until the sensor receives data for the first time.
 - This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the **local system** (on every node, if on a cluster probe), or on the system running the [remote probe](#) ³⁷⁰⁹. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Remote PowerShell

The Windows Updates Status (PowerShell) sensor uses PowerShell commands. To monitor devices with this sensor, **Remote PowerShell** access has to be enabled on the target computer. Also ensure that you have installed **PowerShell 3.0** or later on both your probe machine and target system.

⚠ In larger environments, the default memory limit for the remote shell might be insufficient and you might see the error message "The WSMAN provider host process did not return a proper response". In this case, increase the memory limit for Remote PowerShell. For more details, see this Knowledge Base article: [How can I increase memory for Remote PowerShell?](#)

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SPECIFIC

Port Enter the number of the port to which this sensor connects. Please enter an integer value. The default port is **5985**.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

 This sensor type has a fixed minimum scanning interval for performance reasons. You cannot run the sensor in shorter intervals than this minimum interval. Consequently, shorter scanning intervals as defined in [System Administration—Monitoring](#)³³⁵⁵ are not available for this sensor.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: Facing issues with the Windows Update Status Sensor—Can you help me?

- <https://kb.paessler.com/en/topic/71899>

Knowledge Base: How do I enable and use remote commands in Windows PowerShell?

- <https://kb.paessler.com/en/topic/44453>

Knowledge Base: My PowerShell sensor returns an error message. What can I do?

- <https://kb.paessler.com/en/topic/59473>

Knowledge Base: "No Logon Servers Available" when Using PowerShell Sensors

- <https://kb.paessler.com/en/topic/59745>

Knowledge Base: How can I increase memory for Remote PowerShell?

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
229 Windows Updates Status (Powershell) Sensor

- <https://kb.paessler.com/en/topic/61922>

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[3160] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[3170] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

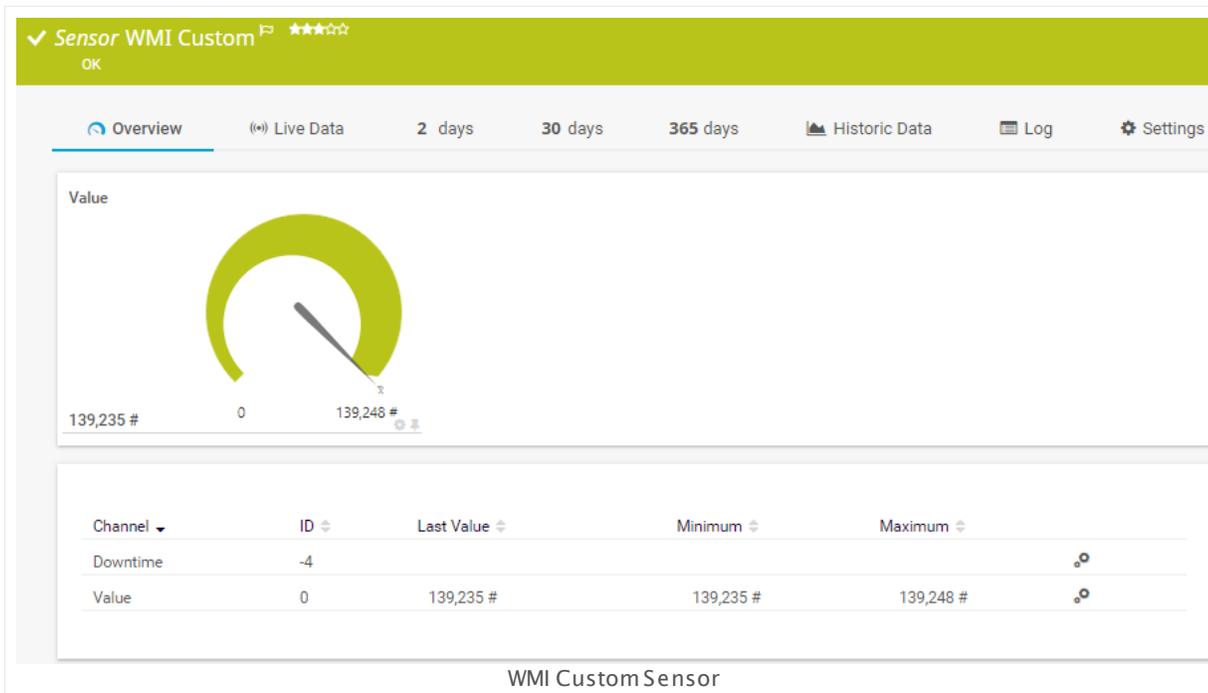
7.8.230 WMI Custom Sensor

The WMI Custom sensor performs a custom query via Windows Management Instrumentation (WMI) and monitors numerical values (integers and floats).

- It shows the retrieved value.

i Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on. If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node. Save the file with the query into the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. See the section [Data Storage](#) for more information about how to find this path.

i If your WQL query returns strings, use the [WMI Custom String Sensor](#).



Sensor in Other Languages

Dutch: **WMI (Klant Specifiek)**, French: **WMI (personnalisé)**, German: **WMI (Benutzerdef.)**, Japanese: **WMI** ? ? ? ? , Portuguese: **WMI customizado**, Russian: **Нестандартный WMI**, Simplified Chinese: **WMI** ? ? ? , Spanish: **WMI personalizado**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)¹²⁵. Above this number, please consider using multiple [Remote Probes](#)³⁷⁰⁹ for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)³⁵⁰⁷.
- Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
- Knowledge Base: [How do I create a WMI Custom sensor?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CUSTOM QUERY SPECIFIC

Channel Name Enter a name for the channel in which PRTG shows the received data. This name will be displayed in graphs and tables. Please enter a string.

 You can change the name later in the sensor's [channel settings](#)³¹⁶⁰.

WQL File Select a file from the list that this sensor will use. The sensor executes it with every scanning interval. The menu contains WQL scripts from the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. Please store your script there.

If used on a remote probe, you must store the file on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node. For more information on how to find this path, see section [Data Storage](#)³⁷³⁴.

 Your query must return an integer or float value. Strings are not supported, use the [WMI Custom String Sensor](#)²⁸⁷⁷ in this case.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CUSTOM QUERY SPECIFIC

Namespace	Enter the namespace for the query.
-----------	------------------------------------

CUSTOM QUERY SPECIFIC

WQL File	<p>Shows the WQL file that this sensor executes with every scanning interval. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p> <p> Your query must return an integer or float value. Strings are not supported, use the WMI Custom String Sensor²⁸⁷⁷ in this case.</p>
Placeholder <#PH1>	<p>In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH1> or leave the field empty.</p>
Placeholder <#PH2>	<p>In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH2> or leave the field empty.</p>
Placeholder <#PH3>	<p>In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH3> or leave the field empty.</p>
If Value Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none">▪ Ignore changes (default): The sensor takes no action on change.▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification³¹⁷⁰ whenever the sensor value changes.
Unit String	<p>Enter a unit for the data that the sensor receives from your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.</p>
Multiplication	<p>Define a multiplier for the received values. The default value is 1 to not change received values. Please enter an integer value.</p>
Division	<p>Define a divisor for the received values. The default value is 1 to not change received values. Please enter an integer value.</p>

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

- [Additional Sensor Types \(Custom Sensors\)](#)³¹⁵⁵

Knowledge Base: How do I properly configure a WMI Custom Sensor?

- <https://kb.paessler.com/en/topic/163>

Knowledge Base: How do I create a WMI Custom Sensor?

- <https://kb.paessler.com/en/topic/2743>

Knowledge Base: Which WQL queries are used by PRTG's WMI sensors?

- <https://kb.paessler.com/en/topic/8783>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

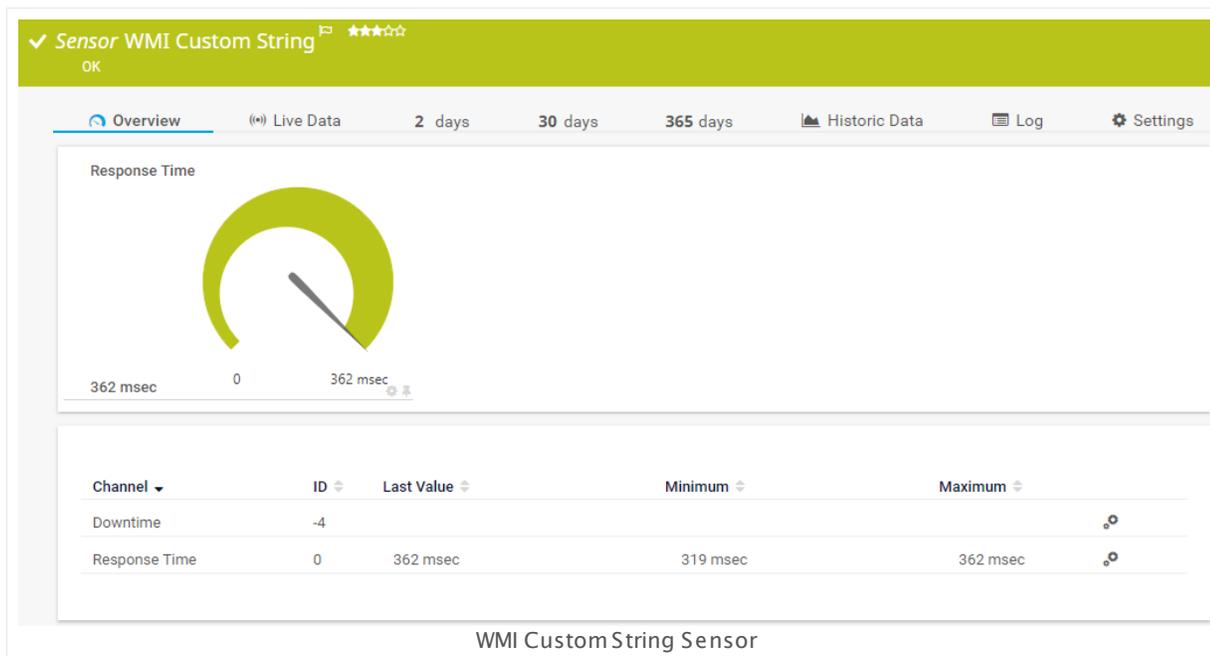
7.8.231 WMI Custom String Sensor

The WMI Custom String sensor performs a custom string query via Windows Management Instrumentation (WMI).

- It shows the retrieved string value in the sensor message.
- It also shows the response time.

i Your Windows Management Instrumentation Query Language (WQL) query code must be stored in a file on the system of the probe the sensor is created on. If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node. Save the file with the query into the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. See the section [Data Storage](#) for more information about how to find this path.

i If your WQL query returns numerical values, use the [WMI Custom Sensor](#).



Sensor in Other Languages

Dutch: **WM Aangepaste Tekenreeks**, French: **Chaîne personnalisée WMI**, German: **WMI Text (benutzerdef.)**, Japanese: **WMI ? ? ? ? ? ?**, Portuguese: **Sequência de caracteres personalizada WMI**, Russian: **Нестандартная строка WMI**, Simplified Chinese: **WMI ? ? ? ? ? ?**, Spanish: **WMI cadena personalizada**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
- Knowledge Base: [Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?](#)
- Knowledge Base: [How do I create a WMI Custom Sensor?](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

CUSTOM QUERY SPECIFIC

WQL File

Select a file that will be used for this sensor from the list. The sensor will execute it with every scanning interval.

The list contains WQL scripts from the **\Custom Sensors\WMI WQL scripts** subfolder of your PRTG installation. Please store your script there. If used on a remote probe, the file must be stored on the system running the remote probe. If used on a cluster probe, you must store the file on all servers running a cluster node! For more information on how to find this path, see section [Data Storage](#)^[3734].

 If your WQL query returns integers or floats, use the [WMI Custom Sensor](#)^[2807] to not only show the returned value in the sensor message, but also monitor the value in a sensor channel.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

CUSTOM QUERY SPECIFIC

Namespace	Enter the namespace for the query.
WQL File	<p>Shows the name of the file that this sensor uses. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p> <p>i If your WQL query returns integers or floats, use the WMI Custom Sensor to not only show the returned value in the sensor message, but also monitor the value in a sensor channel.</p>

CUSTOM QUERY SPECIFIC

Placeholder <#PH1>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH1> or leave the field empty.
Placeholder <#PH2>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH2> or leave the field empty.
Placeholder <#PH3>	In your WQL script, you can use up to three placeholders that you can assign a value to in this field. Enter a string for variable <#PH3> or leave the field empty.
Unit String	Enter a unit for the data that will be received by your script. This is for displaying purposes only. The unit will be displayed in graphs and tables. Please enter a string.
If Value Changes	<p>Define what this sensor will do when the sensor value changes. You can choose between:</p> <ul style="list-style-type: none"> ▪ Ignore changes (default): The sensor takes no action on change. ▪ Trigger 'change' notification: The sensor sends an internal message indicating that its value has changed. In combination with a Change Trigger, you can use this mechanism to trigger a notification <small>[3770]</small> whenever the sensor value changes.
Response Must Include	Define which string must be part of the data that is received from the WMI object. You can either enter plain text or a Regular Expression <small>[3704]</small> . If the data does not include the search pattern, the sensor will show a Down status <small>[195]</small> . Please enter a string or leave the field empty.
Response Must Not Include	Define which string must not be part of the data that is received from the WMI object. You can either enter plain text or a Regular Expression <small>[3704]</small> . If the data does include the search pattern, the sensor will show a Down status <small>[195]</small> . Please enter a string or leave the field empty.
For Keyword Search Use	<p>Define the format of the search expression you entered above.</p> <ul style="list-style-type: none"> ▪ Plain Text: Search for the string as plain text. The characters * and ? work here as placeholders, whereas * stands for no or any number of characters and ? stands for exactly one character (as known from Windows search). This behavior cannot be disabled, so the literal search for these characters is not possible with plain text search.

CUSTOM QUERY SPECIFIC

- **Regular Expression:** Handle the search pattern as a [Regular Expression](#)^[3704].

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

Maximum Length of String

Define the maximum allowed length of the string that will be received from the WMI object. If it is longer than this value, the sensor will show a **Down status**^[195]. Please enter an integer value or leave the field empty.

Extract Number Using Regular Expression

Define if you want to filter out a numeric value from the string received from the WMI object. You can convert this into a float value to use it with channel limits (see [Sensor Channels Settings](#)^[3160]).

- **No extraction:** Do not extract a float value. Use the result as a string value.
- **Extract a numeric value using a regular expression:** Use a regular expression to identify a numeric value in the string and convert it to a float value. Define below.
 See also the [example](#)^[2887] below.

Regular Expression

This setting is only visible if number extraction is enabled above. Enter a [Regular Expression](#)^[3704] to identify the numeric value you want to extract from the string returned by the WMI object. You can use capturing groups here.

Make sure the expression returns numbers only (including decimal and thousands separators). The result will be further refined by the settings below.

 PRTG supports **PCRE** regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)^[3704].

Index of Capturing Group

This setting is only visible if number extraction is enabled above. If your regular expression uses capturing groups, specify which one will be used to capture the number. Please enter an integer value or leave the field empty.

Decimal Separator

This setting is only visible if number extraction is enabled above. Define which character to use as decimal separator for the number extracted above. Please enter a string or leave the field empty.

CUSTOM QUERY SPECIFIC

- Thousands Separator** This setting is only visible if number extraction is enabled above. Define which character to use as thousands separator for the number extracted above. Please enter a string or leave the field empty.
- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 📁 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 - ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
- 📘 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - 📘 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

Example: Number Extraction with Regular Expression

 If you want to extract a number in the response string using a regular expression, please note that the index for captures in this sensor is based on **1 (not on 0)**. Furthermore, capturing groups are not created automatically. The example below will illustrate this issue.

Consider the following string as returned by a request for CPU usage:

```
5 Sec (3.49%), 1 Min (3.555%), 5 Min (3.90%)
```

Assuming you would like to filter for the number **3.555**, that is the percentage in the second parentheses. Then enter the following regex in the **Regular Expression** field:

```
(\d+\.\d+).*?(\d+\.\d+).*?(\d+\.\d+)
```

As **Index of Capturing Group** enter **3**. This will extract the desired number **3.555**.

The index has to be 3 in this case because the capturing groups here are the following:

- Group 1 contains 3.49%, 1 Min (3.555), 5 Min (3.90)
- Group 2 contains 3.49
- Group 3 contains 3.555
- Group 4 contains 3.90

Please keep in mind this note about index and capturing groups when using number extraction.

 It is not possible to match an empty string with the PRTG regex sensor search.

 PRTG supports PCRE regex. You cannot use regex options or flags. For more details, see manual section [Regular Expressions](#)³⁷⁰⁴.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Knowledge Base: How do I create a WMI Custom Sensor?

- <https://kb.paessler.com/en/topic/2743>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

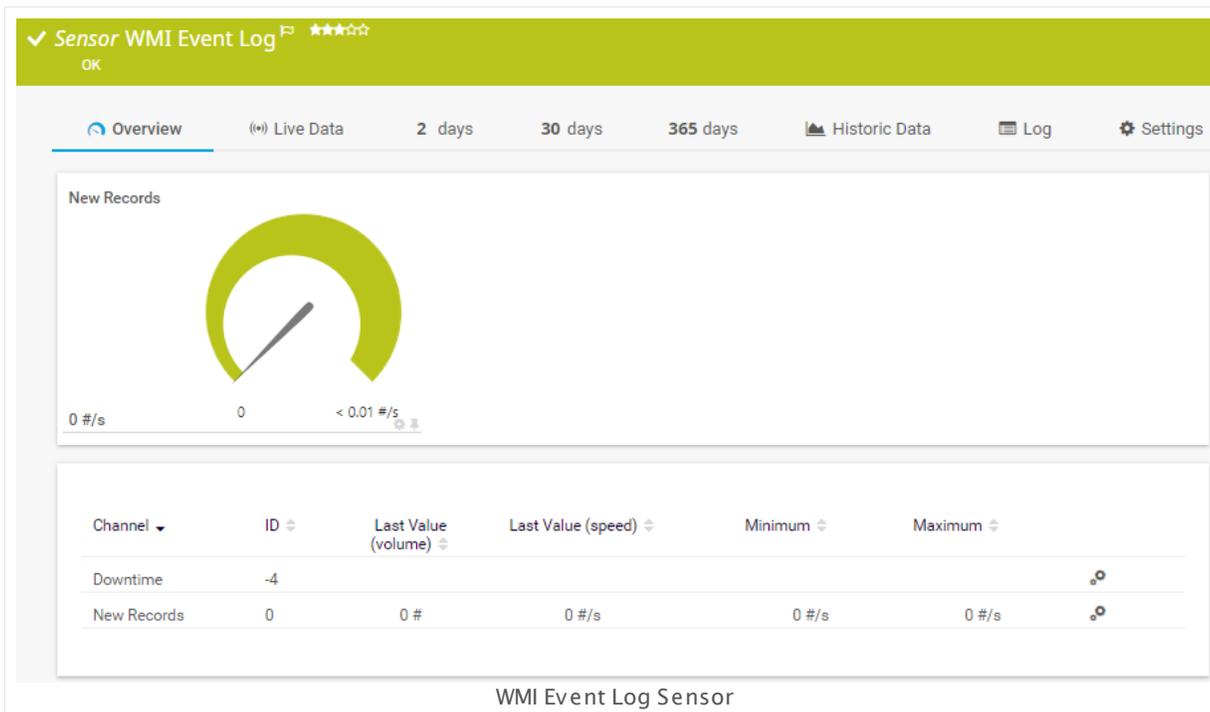
7.8.232 WMI Event Log Sensor

The WMI Event Log sensor monitors a specific Windows logfile using Windows Management Instrumentation (WMI).

- It shows the number of new records per second.

You can set the sensor to a desired status individually according to a new event log entry.

 For details and how to find out the correct filter, see the Knowledge Base: [My Event Log sensor ignores changes in the event log. What can I do?](#)



Sensor in Other Languages

Dutch: **WMI Logboek**, French: **Log des événements WMI**, German: **WMI Ereignisprotokoll**, Japanese: **WMI** ? ? ? ? ? , Portuguese: **Log de eventos WMI**, Russian: **Журнал событий WMI**, Simplified Chinese: **WMI** ? ? ? ? , Spanish: **WMI event log**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
- Knowledge Base: [My Event Log sensor ignores changes in the event log. What can I do?](#)
- Knowledge Base: [How can I configure sensors using speed limits to keep the status for more than one interval?](#)
- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logfiles you want to monitor. PRTG will create one sensor for each log you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI EVENT LOG MONITOR

Log File	The Windows event log provides several different logfiles. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
----------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI EVENT LOG MONITOR

Log File	Shows the Windows logfile that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result.

WMI EVENT LOG MONITOR

- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

FILTER EVENT LOG ENTRIES

Event Type	<p>Specify the type of event that this sensor processes. Other event types cannot be processed. Choose between the following event types:</p> <ul style="list-style-type: none"> ▪ Any ▪ Error ▪ Warning ▪ Information ▪ Security Audit Success ▪ Security Audit Failure
Filter by Source	<p>Filter all received events for a certain event source. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none"> • Off: Do not filter by event source. • On: Enable filtering by event source.
Filter Type	<p>This field is only visible if you enable source filtering above. Choose between:</p> <ul style="list-style-type: none"> • Include Filter: Include the specified value and disregard all other values. • Exclude Filter: Exclude the specified value and regard all other values.

FILTER EVENT LOG ENTRIES

Match String (Event Source)	This field is only visible if you enable source filtering above. Enter an event source that you want to filter for. Depending on the kind of filter, the event source is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by ID	<p>Filter all received events for a certain event ID. If you enable this option, this sensor processes only messages that match the defined value(s). Choose between:</p> <ul style="list-style-type: none"> • Off: Do not filter by event ID. • On: Enable filtering by event ID.
Filter Type	<p>This field is only visible if you enable ID filtering above. Choose between:</p> <ul style="list-style-type: none"> • Include Filter: Include the specified value and disregard all other values. • Exclude Filter: Exclude the specified value and regard all other values.
Match Values (Event ID)	<p>This field is only visible if you enable ID filtering above. Enter an event ID that you want to filter for. Depending on the kind of filter, the event ID is processed (Include Filter) or not processed (Exclude Filter).</p> <p> The Event Log (Windows API) Sensor⁷⁶¹ supports more than one event ID. Using this sensor type, you can enter a comma-separated list of event IDs to filter for more than one ID.</p> <p> The WMI Event Log Sensor²⁸⁹³ supports filtering for only one ID.</p>
Filter by Category	<p>Filter all received events for a certain event category. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none"> • Off: Do not filter by event category. • On: Enable filtering by event category.
Filter Type	<p>This field is only visible if you enable category filtering above. Choose between:</p> <ul style="list-style-type: none"> • Include Filter: Include the specified value and disregard all other values. • Exclude Filter: Exclude the specified value and regard all other values.

FILTER EVENT LOG ENTRIES

Match String (Event Category)	This field is only visible if you enable category filtering above. Enter a category that you want to filter for. Depending on the kind of filter, the event category is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by User	Filter all received events for a certain event user. If you enable this option, this sensor only processes messages that match the defined value. Choose between: <ul style="list-style-type: none">• Off: Do not filter by event user.• On: Enable filtering by event user.
Filter Type	This field is only visible if you enable user filtering above. Choose between: <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event User)	This field is only visible if you enable user filtering above. Enter a username that you want to filter for. Depending on the kind of filter, the event user is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.
Filter by Computer	Filter all received events for a certain event computer. If you enable this option, this sensor only processes messages that match the defined value. Choose between: <ul style="list-style-type: none">• Off: Do not filter by event computer.• On: Enable filtering by event computer.
Filter Type	This field is only visible if you enable computer filtering above. Choose between: <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event Computer)	This field is only visible if you enable computer filtering above. Enter a computer name that you want to filter for. Depending on the kind of filter, the event computer is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.

FILTER EVENT LOG ENTRIES

Filter by Message	<p>Filter all received events for a certain event message. If you enable this option, this sensor only processes messages that match the defined value. Choose between:</p> <ul style="list-style-type: none">• Off: Do not filter by event message.• On: Enable filtering by event message.
Filter Type	<p>This field is only visible if you enable message filtering above. Choose between:</p> <ul style="list-style-type: none">• Include Filter: Include the specified value and disregard all other values.• Exclude Filter: Exclude the specified value and regard all other values.
Match String (Event Message)	<p>This field is only visible if you enable message filtering above. Enter a message that you want to filter for. Depending on the kind of filter, the event message is processed (Include Filter) or not processed (Exclude Filter). Please enter a string.</p>

i For the **WMI Event Log Sensor**, you can use the percent sign (%) as placeholder for any or no character (as known from the asterisk sign (*) in Windows search) in combination with a substring. For example, you can enter %RAS% for any event source containing the string RAS.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p>i You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none">▪ Show channels independently (default): Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁸⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

Knowledge Base: My Event Log sensor ignores changes in the event log. What can I do?

- <https://kb.paessler.com/en/topic/59803>

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

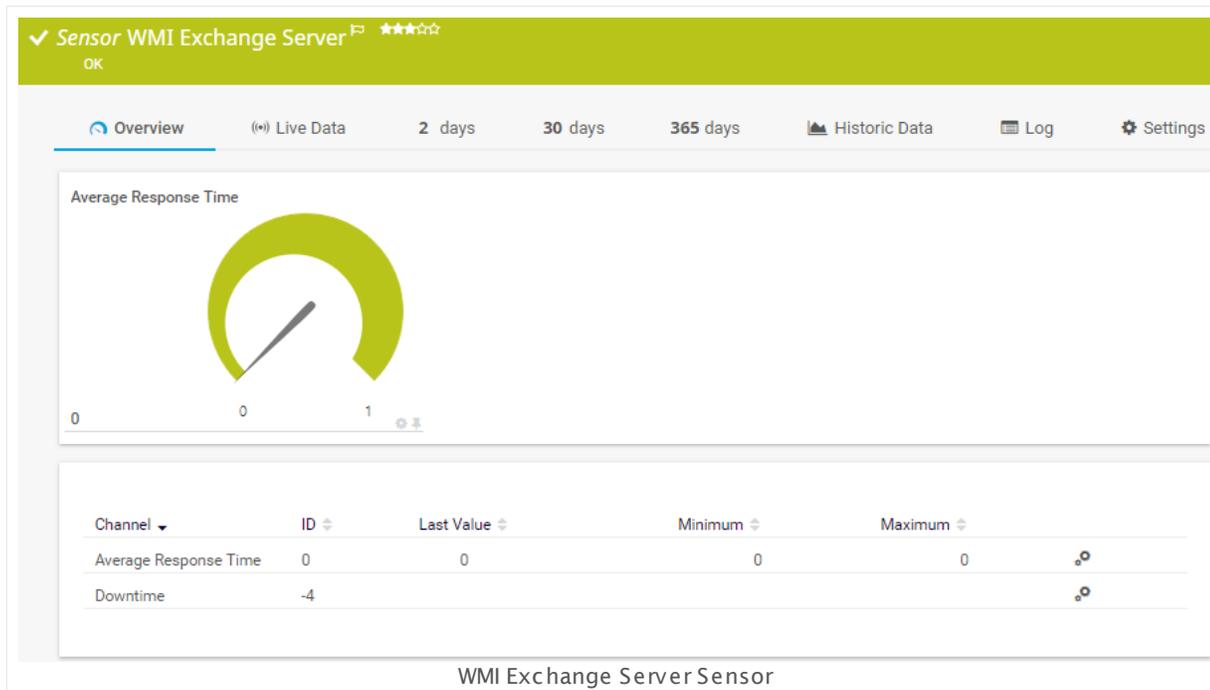
7.8.233 WMI Exchange Server Sensor

The WMI Exchange Server sensor monitors a Microsoft Exchange Server 2003, 2007, 2010, or 2013 using Windows Management Instrumentation (WMI).

It can show the following:

- Queue size
- Average delivery time
- Logon operations per second
- Sent, delivered, and submitted messages per second
- Messages queued for submission
- Remote Procedure Call (RPC) packets operations per second
- RPC latency, requests, and slow packets
- RPC sent, slow, outstanding, and failed requests (store interface)
- Read and write bytes RPC clients per second
- Number of active and anonymous users
- Database page faults per second
- Log record stalls per second
- Log threads waiting
- Database cache size in bytes and miss in percent
- Current unique users (OWA)
- Average response time (OWA)

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

WMI Exchange Server, French: **Exchange Server WMI**, German: **WMI Exchange-Server**, Japanese: **WMI Exchange** ? ? ? , Portuguese: **Exchange Server WMI**, Russian: **WMI Exchange Server**, Simplified Chinese: **WMI Exchange** ? ? ? , Spanish: **WMI servidor Exchange**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[350].

i Existing former "WMI Exchange Server 2003/2007 Sensors" from previous PRTG versions will continue to monitor your Exchange server in PRTG 9, but newly added Exchange server sensors will be of the "WMI Exchange Server Sensor" type, which is able to monitor Exchange servers regardless of their version.

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) ³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters of the Exchange server you want to monitor. PRTG will create one sensor for each performance counter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

EXCHANGE SERVER DATA READINGS ACCESSIBLE USING WMI

Performance Counter You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The available options depend on your Exchange server configuration. PRTG shows all possible performance counters with name and instance description (if available).

You might be able to select aspects regarding:

- **SMTP Server:** Queue Lengths
- **MSExchangeIS Mailbox:** Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS Public:** Queue Sizes, Delivery Times, Operations, Messages
- **MSExchangeIS:** Packets, Operations, Clients, Latency, Requests, Users
- **MS Exchange RPC Client Access:** Active User Count, User Count, Connection Count
- **MS Exchange OWA:** Current Unique Users, Average Response Time

 Depending on your Exchange server version, not all counters might be available.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	
Counter	
Time Stamp	
Time Frequency	
Counter Type	
Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none"> ▪  For more information on how to find the folder used for storage, see section Data Storage. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.234 WMI Exchange Transport Queue Sensor

The WMI Exchange Transport Queue sensor monitors the length of transport queues of a Microsoft Exchange Server 2003, 2007, 2010, or 2013 using Windows Management Instrumentation (WMI). It shows the same information as shown in Windows System Monitor [perfmon](#).

This sensor can show the following:

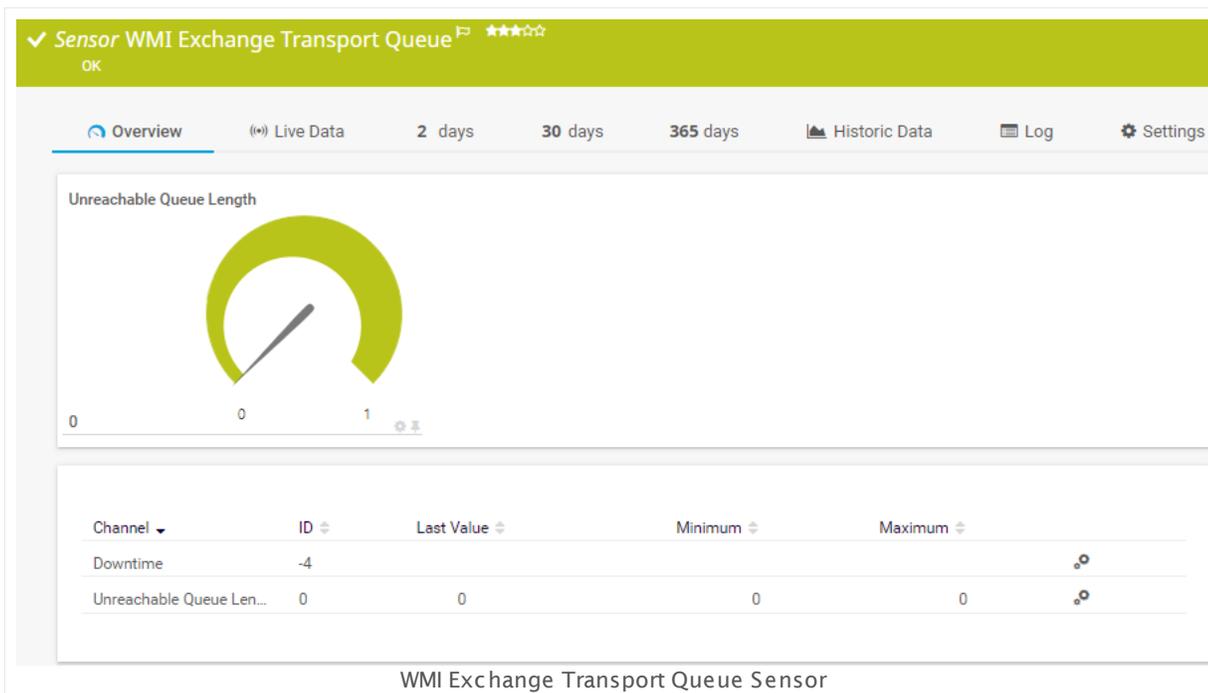
- Active Mailbox Delivery Queue Length
- Active Non-Smtp Delivery Queue Length
- Active Remote Delivery Queue Length
- Aggregate Delivery Queue Length (All Queues)
- Aggregate Shadow Queue Length
- Categorizer Job Availability
- Items Completed Delivery Per Second
- Items Completed Delivery Total
- Items Deleted By Admin Total
- Items Queued For Delivery Expired Total
- Items Queued for Delivery Per Second
- Items Queued For Delivery Total
- Items Resubmitted Total
- Largest Delivery Queue Length
- Messages Completed Delivery Per Second
- Messages Completed Delivery Total
- Messages Completing Categorization
- Messages Deferred Due To Local Loop
- Messages Deferred during Categorization
- Messages Queued For Delivery
- Messages Queued for Delivery Per Second
- Messages Queued For Delivery Total
- Messages Submitted Per Second
- Messages Submitted Total
- Poison Queue Length
- Retry Mailbox Delivery Queue Length
- Retry Non-Smtp Delivery Queue Length
- Retry Remote Delivery Queue Length

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings 234 WMI Exchange Transport Queue Sensor

- Shadow Queue Auto Discards Total
- Submission Queue Items Expired Total
- Submission Queue Length
- Unreachable Queue Length

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.

 For an explanation of the transport queue types, see the Knowledge Base: [Types of Transport Queues in Microsoft Exchange](#)



Sensor in Other Languages

Dutch: **WMI Exchange Transport Wachtrij**, French: **File d'attente de transport WMI Exchange**, German: **WMI Exchange Transportwarteschlange**, Japanese: **WMI Exchange ? ? ?**, Portuguese: **Fila de transporte do Exchange WMI**, Russian: **Очередь транспорта WMI Exchange**, Simplified Chinese: **WMI Exchange ? ? ? ?**, Spanish: **Cola de transporte WMI Exchange**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
- Knowledge Base: [Types of Transport Queues in Microsoft Exchange](#)

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the transport queues you want to monitor. PRTG will create on sensor for each queue you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI EXCHANGE TRANSPORT QUEUE SPECIFIC

MSExchangeTransport Queues You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

The available options depend on your Exchange server configuration. PRTG shows all possible queues with names and instance descriptions (if available).

 For performance reasons, we recommend that you only select necessary items!

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	

READINGS ACCESSIBLE USING WMI

Counter

Time Stamp

Time Frequency

Counter Type

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#).

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Types of Transport Queues in Microsoft Exchange

- <https://kb.paessler.com/en/topic/55413>

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

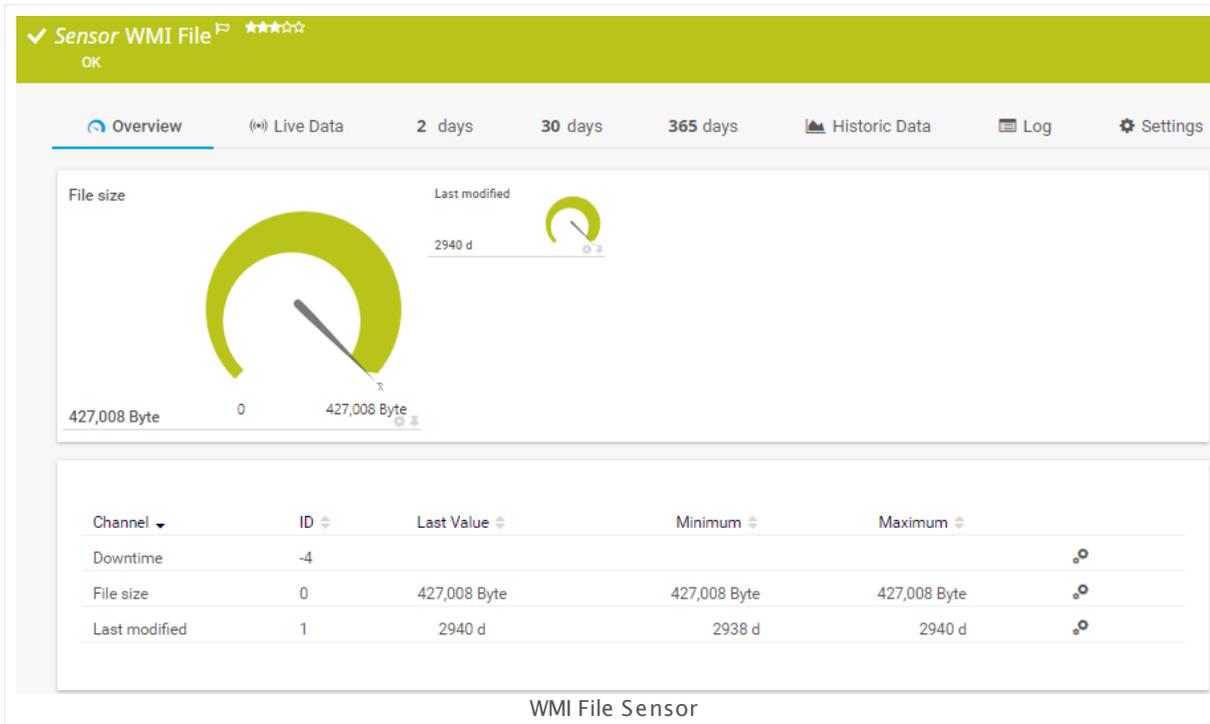
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.235 WMI File Sensor

The WMI File sensor monitors a file using Windows Management Instrumentation (WMI).

It shows the following:

- File size
- Elapsed time since its last modification



Sensor in Other Languages

Dutch: **WMI Bestand**, French: **Fichier WMI**, German: **WMI Datei**, Japanese: **WMI ? ? ? ?**, Portuguese: **Arquivo WMI**, Russian: **Файл WMI**, Simplified Chinese: **WMI ? ?**, Spanish: **WMI archivo**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI FILE MONITOR

- File Name** Enter the name of the file that you want to monitor with the sensor. Enter the full local path. The file must exist on the computer your local or remote probe is running on. UNC paths are not allowed here. For example, when you create this sensor on a device under the local probe, the file has to be accessible on the local system.
- If Timestamp Changes** Define what to do when the timestamp of the file changes. You can choose between:
- **Ignore changes (default):** The sensor will not take action on change.
 - **Trigger 'change' notification:** The sensor will send an internal message indicating that the timestamp has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³¹⁷⁰ whenever the timestamp changes.

DEBUG OPTIONS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

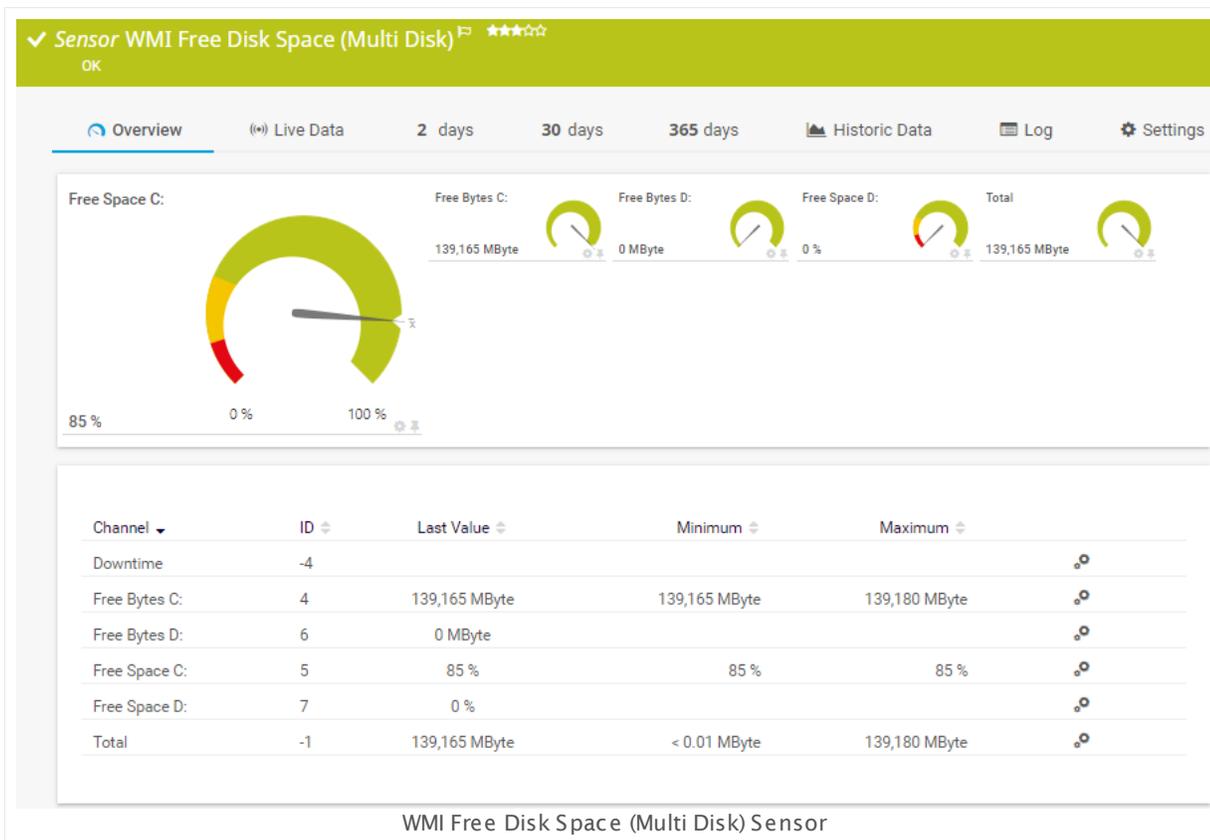
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.236 WMI Free Disk Space (Multi Disk) Sensor

The WMI Free Disk Space (Multi Disk) sensor monitors the free disk space of one or multiple drive(s) using Windows Management Instrumentation (WMI).

It shows the following:

- Free disk space in percent and bytes for each disk
 - Disk space of a system in total
- i** The sensor monitors logical partitions of a hard or fixed disk drive. PRTG identifies logical disks by their drive letter, such as C.



Sensor in Other Languages

Dutch: **WMI Vrije Schijfruimte (Multi Schijf)**, French: **Capacité du disque WMI (plusieurs fois)**, German: **WMI Laufwerkskapazität (mehrf.)**, Japanese: **WMI ? ? ? ? ? ? ? ? (? ? ? ? ? ?)**, Portuguese: **Espaço livre em disco da WMI (vários discos)**, Russian: **Свободное дисковое пространство WMI (на нескольких дисках)**, Simplified Chinese: **WMI ? ? ? ? ? ? (? ? ? ?)**, Spanish: **WMI disco libre (discos múltiples)**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI DISK FREE CONFIGURATION

Drive Select the drive(s) you want to monitor from the dropdown menu. We recommend that you use the default value.

You can choose **All** to monitor all available drives, or you can choose one specific drive letter to monitor a single drive only. The data in the dropdown menu may also contain drive letters that do not exist on your device. The drive setting cannot be changed once the sensor is created.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI DISK FREE CONFIGURATION

Drive	Shows the drive(s) that this sensor monitors. This is either All or a specific drive letter. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-------	--

SET LIMITS CHECKED AGAINST ALL DISKS

In this section you can set limits that are valid for all channels and all drives. By entering limits, you can define when the sensor will enter a **Warning** or **Down status**^[195], depending on the data provided by all drives that this sensor monitors. If you want to individually define limits for separate channels, please use the limit settings in the [Sensor Channels Settings](#)^[3160].

i All limits that you define here are valid in addition to the limits defined in the particular **Channel** settings! The limits are valid simultaneously, so the first limit that is breached applies.

Percentage Limit Check Enable or disable a limit check for the free space in percentage channels of all drives. By default, percentage limits are enabled with lower warning and lower error limit. Choose between:

- **Only use the limits in the settings of the percentage channels:** Do not define sensor limits that are valid for all percentage channels. The sensor only uses limits that you define in the settings of the particular "free space in percent" channels to determine the status.
- **Use the limits of both the sensor and the channel settings:** Define limits for the sensor that are valid for all drives (percentage channels). Additional fields appear below. The sensor enters a **Warning** or **Down** status when free space limits are undercut or overrun.

Upper Error Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Down** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

i The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)^[3160]. The limits set here and in the channel settings are valid simultaneously!

Upper Warning Limit This field is only visible if you enable percentage limit check above. Specify an upper limit in percent for a **Warning** status. If the free disk space of one of your drives overruns this percent value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

i The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)^[3160]. The limits set here and in the channel settings are valid simultaneously!

SET LIMITS CHECKED AGAINST ALL DISKS

Lower Warning Limit	<p>This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a Warning status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to warning. Please enter an integer value or leave the field empty.</p> <p> The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!</p>
Lower Error Limit	<p>This field is only visible if you enable percentage limit check above. Specify a lower limit in percent for a Down status. If the free disk space of one of your drives undercuts this percent value, the sensor switches to Down. Please enter an integer value or leave the field empty.</p> <p> The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!</p>
Size Limit Check	<p>Enable or disable a limit check for the free bytes channels of all drives. By default, byte size limits are not enabled for drives. Choose between:</p> <ul style="list-style-type: none">• Only use the limits in the settings of the byte size channels: Do not define sensor limits that are valid for all byte size channels. The sensor only uses limits that you define in the settings of the particular free space in bytes channels to determine the status.• Use the limits of both the sensor and the channel settings: Define limits for the sensor that are valid for all drives (byte size channels). Additional fields appear below. The sensor enters a Warning or Down status when free space limits are undercut or overrun.
Upper Error Limit	<p>This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor will switch to Down. Please enter an integer value or leave the field empty.</p> <p> The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the Sensor Channels Settings³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!</p>

SET LIMITS CHECKED AGAINST ALL DISKS

Upper Warning Limit This field is only visible if you enable byte limit check above. Specify an upper limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives overruns this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Warning Limit This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Warning**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Lower Error Limit This field is only visible if you enable byte limit check above. Specify a lower limit. Use the same unit as shown by the free bytes channels of this sensor (by default this is MByte). If the free disk space of one of your drives undercuts this bytes value, the sensor switches to **Down**. Please enter an integer value or leave the field empty.

 The limits set here are valid for all channels of this sensor. You can additionally set individual limits for each sensor channel in the [Sensor Channels Settings](#)³¹⁶⁰. The limits set here and in the channel settings are valid simultaneously!

Alarm on Missing/Removed Disk If a monitored disk is removed or not found, values are set to zero. Select the alarming approach in this case. Choose between:

- **Deactivate alarm (default):** Select this option if you do not want an alarm for a removed disk.
- **Activate alarm:** Select this option if you want to be alerted if a monitored disk is removed.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.237 WMI HDD Health Sensor

The WMI HDD Health sensor connects to the parent device via Windows Management Instrumentation (WMI) and monitors the health of IDE disk drives on the target system, using Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.). This is built into most modern IDE hard disk drives.

It can show the following, among others:

- Read Error Rate
- Spin-Up Time
- Start/Stop Count
- Reallocated Sectors Count
- Seek Error Rate
- Power-On Hours
- Spin Retry Count
- Calibration Retry Count
- Power Cycle Count
- Power-off Retract Count
- Load Cycle Count
- Temperature Celsius
- Reallocation Event Count
- Current Pending Sector Count
- Uncorrectable Sector Count
- UltraDMA CRC Error Count
- Write Error Rate
- Transfer Error Rate
- Total LBAs Written
- Total LBAs Read

Which channels the sensor actually shows might depend on the monitored device and the sensor setup. The channel names indicate the ID of the S.M.A.R.T. attribute, followed by a colon, and the typical meaning of the channel. The sensor can also show other attributes that the target device returns, but some channels will have the name **Unknown Channel**. This happens if PRTG cannot match the ID of a found attribute with an internally defined channel name.

 Some vendors do not agree on attribute definitions and define meanings other than the common one.

Every attribute of a disk assumes a value. PRTG shows these attributes as channels with their last, minimum, and maximum value. These channel values change over time and indicate the disk health—higher values correspond to a better health. The disk's attributes come with a threshold, defined by the manufacturer of the drive. If a channel value is lower than this threshold, the sensor will automatically show a **Warning status**^[195]. This indicates that the S.M.A.R.T. status of the HDD might break soon.

⚠ There are no thresholds defined for some attributes and because of this they cannot be categorized for a status other than **Up**. You can **Define Lookups**^[3693] and use them with affected channels to get the desired status for a return value.

✓ Sensor WMI HDD Health ☆☆☆☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Channel	ID	Last Value	Minimum	Maximum	
001: Read Error Rate	2	119 #	119 #	119 #	⚠
003: Spin-Up Time	3	98 #	98 #	98 #	⚠
004: Start/Stop Count	4	83 #	83 #	83 #	⚠
005: Reallocated Sectors...	5	100 #	100 #	100 #	⚠
007: Seek Error Rate	6	80 #	80 #	80 #	⚠
009: Power-On Hours	7	84 #	84 #	84 #	⚠
010: Spin Retry Count	8	100 #	100 #	100 #	⚠
012: Power Cycle Count	9	92 #	92 #	92 #	⚠
183: SATA Downshift Err...	10	100 #	100 #	100 #	⚠
184: End-to-End error / IO...	11	100 #	100 #	100 #	⚠

WMI HDD Health Sensor

Sensor in Other Languages

Dutch: **WMI HDD Status**, French: **État WMI HDD**, German: **WMI Laufwerkszustand**, Japanese: **WMI HDD ? ? ?**, Portuguese: **Funcionamento do HD WMI**, Russian: **Работоспособность жесткого диска WMI**, Simplified Chinese: **WMI ? ? ? ? ?**, Spanish: **Salud de disco duro WMI**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
 - Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)¹²⁵. Above this number, please consider using multiple [Remote Probes](#)³⁷⁰⁹ for load balancing.
 - For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)³⁵⁰⁷.
 - This sensor officially requires Windows 7 or later on the target machine that holds the hard disk drives you want to monitor. The sensor may not work reliably if the target machine runs on Windows 2003, Windows XP, or Windows Vista. Due to a known bug in those systems, the sensor may not be able to detect available hard disk drives.
 - The values that this sensor shows can vary depending on how a vendor handles S.M.A.R.T values. See the vendor's documentation for more information.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the IDE disks you want to monitor. PRTG will create one sensor for each IDE device you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SMART SPECIFIC

IDE Devices

You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

 The items shown in the list are specific to the parent device you create the sensor on.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SMART SPECIFIC

Serial No.	Shows the serial number of the monitored disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Size (GB)	Shows the size of the monitored disk in gigabytes. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Name	Shows the name of the monitored disk. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Timeout (Sec.)	Enter a timeout in seconds for the request. If the reply takes longer than this value defines, the sensor will cancel the request and show a corresponding error message. Please enter an integer value. The maximum value is 900 seconds (15 minutes).

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings <small>3311</small>.</p> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> ▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active. ▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window. <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>
Maintenance Begins	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.</p>
Maintenance Ends	<p>This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.</p>
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.238 WMI Logical Disk I/O Sensor

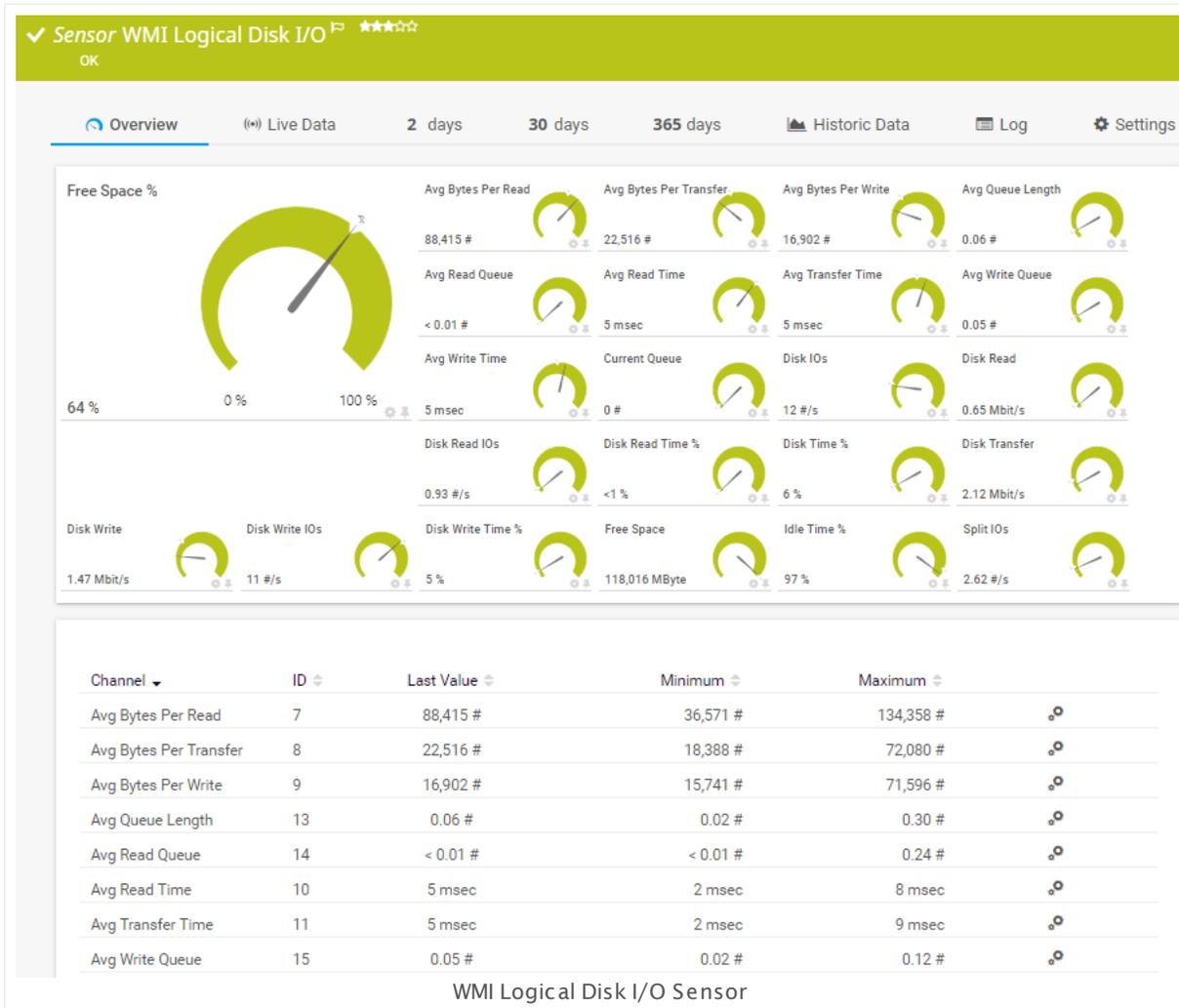
The WMI Logical Disk I/O sensor monitors the disk usage of a logical disk or mount point on a Windows system using Windows Management Instrumentation (WMI).

The sensor provides the following information:

- Free space
- Disk latency
- Disk bandwidth
- Disk queue data
- Disk IOs

 The sensor shows performance data from counters that monitor logical partitions of a hard drive. The system monitor identifies logical disk instances by their identifier, such as **C:**, and the sensor reads the logical disk object in the system monitor and returns the values.

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **WMI Logische Schijf I/O**, French: **E/S du disque logique WMI**, German: **WMI Logischer Datenträger E/A**, Japanese: **WMI ? ? ? ? ? I/O**, Portuguese: **E/S do disco lógico de WMI**, Russian: **Ввод-вывод логического диска WMI**, Simplified Chinese: **WMI ? ? ? ? I/O**, Spanish: **E/S WMI de disco lógico**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.

- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
 - This sensor type supports Windows Server 2008 R2 or later. It will not work on previous Windows versions (Windows Server 2008 or earlier).
 - Currently, this sensor type is in beta status. The methods of operating can change at any **BETA** time, as well as the available settings. Do not expect that all functions will work properly, or that this sensor works as expected at all. Be aware that this type of sensor can be removed again from PRTG at any time.
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the logical disks and mount points you want to monitor. PRTG will create one sensor for each counter you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI LOGICAL DISK I/O SPECIFIC

Logical Disk(s)

Select the logical disks and mount points you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI LOGICAL DISK I/O SPECIFIC

Logical Disk(s)	Shows the logical disk or mount point that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
-----------------	---

DEBUG OPTIONS

Sensor Result	Define what PRTG will do with the sensor results. Choose between:
---------------	---

DEBUG OPTIONS

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
-  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

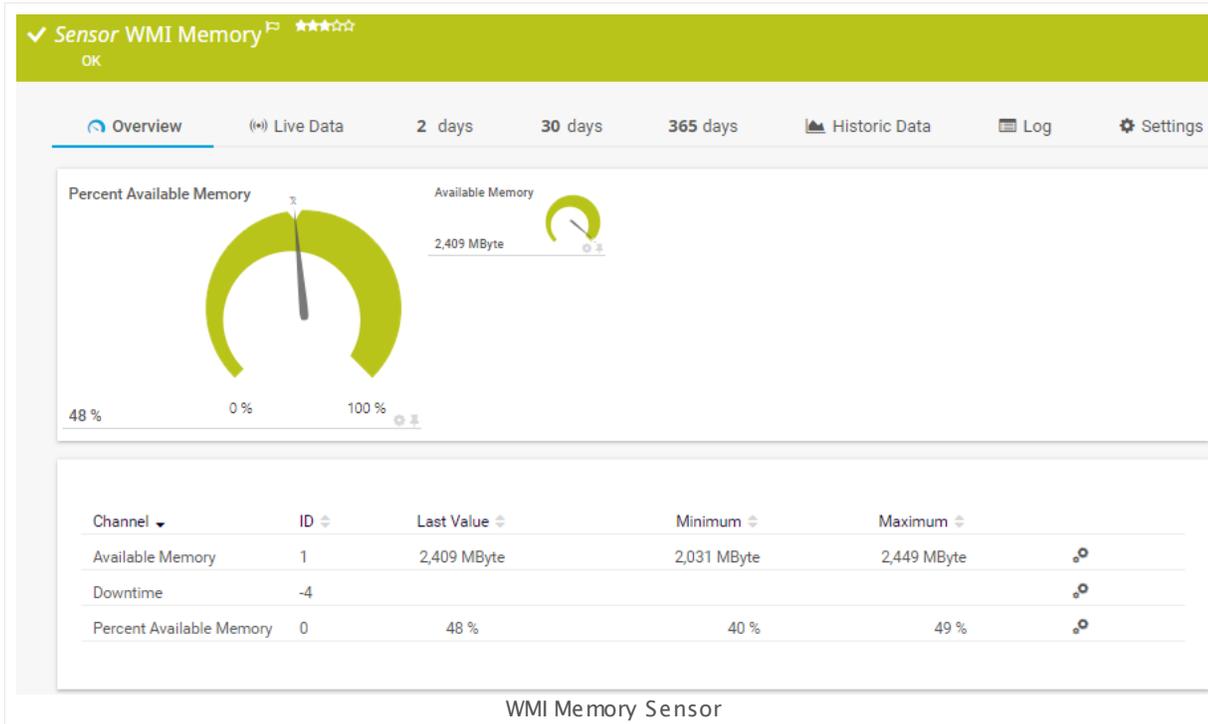
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.239 WMI Memory Sensor

The WMI Memory sensor monitors available (free) system memory on Windows systems using Windows Management Instrumentation (WMI).

- It shows the available memory in percent and bytes.



Sensor in Other Languages

Dutch: **WMI Geheugen**, French: **Mémoire WMI**, German: **WMI Arbeitsspeicher**, Japanese: **WMI** ? ? ? , Portuguese: **Memória de WMI**, Russian: **Память WMI**, Simplified Chinese: **WMI** ? ? , Spanish: **WMI memoria**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

WMI ALTERNATIVE QUERY

Errors and Invalid Data	<p>This is an extended help field only. WMI sensors in PRTG are equipped with the most efficient and accurate WMI queries. However, Microsoft has changed (and will continue to do so in the future) some WMI classes over the various Windows/ServicePack/patchlevel versions, resulting in errors like class not valid or invalid data.</p> <p>Wherever possible, PRTG features an alternative query that might work in your specific configuration. If you keep getting errors for this sensor, please try enabling the alternative query method below.</p>
Alternative Query	<p>Choose the method PRTG uses to query via WMI. For compatibility reasons, you can enable an alternative query method. We recommend that you use the default value. You can choose between:</p> <ul style="list-style-type: none">• Use default (recommended): Use the PRTG standard method to query WMI. This is the best setting in most cases.• Use alternative (if default does not work): Use an alternative method to query WMI. If you keep getting errors with the default setting, try this setting.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.240 WMI Microsoft SQL Server 2005 Sensor (Deprecated)

IMPORTANT NOTICE

This sensor type is deprecated.

Monitoring of Microsoft SQL Server 2005 using PRTG is discontinued. It cannot be monitored with PRTG anymore with the latest updates of SQL Server 2005. The reason for this is a software update delivered by Microsoft in August 2012. The following updates cause this issue:

- **Security Update for SQL Server 2005 Service Pack 4 (KB2716429)**
- **Security Update for SQL Server 2005 Service Pack 4 (KB2716427)**

We have made reasonable effort to fix this from our side but we were unable to. We do not have instructions to circumvent this issue at this time. Please ask the vendor to fix this.

More



Knowledge Base: [Why does my WMI Microsoft SQL Server 2005 Sensor not work anymore?](#)

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.

CHANNEL OVERVIEW

Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.
Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.

CHANNEL OVERVIEW

Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.

- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)¹²⁵. Above this number, please consider using multiple [Remote Probes](#)³⁷⁰⁹ for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)³⁵⁰⁷.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	Enter the version of the SQL Server. Usually, you can keep the default value.

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none"> ▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.
--------------------------	--

SQL COUNTER SPECIFIC

- **Access Methods:** Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).
- **Buffer Manager:** Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.
- **Memory Manager:** Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).
- **Locks:** Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.
- **SQL Statistics:** Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).

Depending on your selection, PRTG creates a sensor with the specified channels.

- ❗ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ❗ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.

BASIC SENSOR SETTINGS

Tags	<p>Enter one or more Tags¹³⁹, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited¹⁴⁰ from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	<p>Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).</p>

SQL SERVER SETTINGS

Service	<p>Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
Name	<p>Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.</p>
WMI Class Name	<p>Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:</p> <ul style="list-style-type: none">▪ Automatic: Choose WMI class automatically. We recommend this setting.▪ Manual: Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.
WMI Class	<p>This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.</p>

SQL SERVER SETTINGS

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

- SQL Performance Counters** Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

 Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

 If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

 If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.241 WMI Microsoft SQL Server 2008 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

241 WMI Microsoft SQL Server 2008 Sensor



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	<p>Enter the version of the SQL Server. Usually, you can keep the default value.</p>

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none">▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.▪ Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).▪ Buffer Manager: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.▪ Memory Manager: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).▪ Locks: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.▪ SQL Statistics: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).
--------------------------	---

SQL COUNTER SPECIFIC

Depending on your selection, PRTG creates a sensor with the specified channels.

- ⓘ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Class Name Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:

- **Automatic:** Choose WMI class automatically. We recommend this setting.
- **Manual:** Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.

WMI Class This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SQL SERVER SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

SQL Performance Counters Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.242 WMI Microsoft SQL Server 2012 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

242 WMI Microsoft SQL Server 2012 Sensor



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	<p>Enter the version of the SQL Server. Usually, you can keep the default value.</p>

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none">▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.▪ Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).▪ Buffer Manager: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.▪ Memory Manager: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).▪ Locks: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.▪ SQL Statistics: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).
--------------------------	---

SQL COUNTER SPECIFIC

Depending on your selection, PRTG creates a sensor with the specified channels.

- ⓘ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Class Name Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:

- **Automatic:** Choose WMI class automatically. We recommend this setting.
- **Manual:** Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.

WMI Class This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SQL SERVER SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

SQL Performance Counters Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.243 WMI Microsoft SQL Server 2014 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

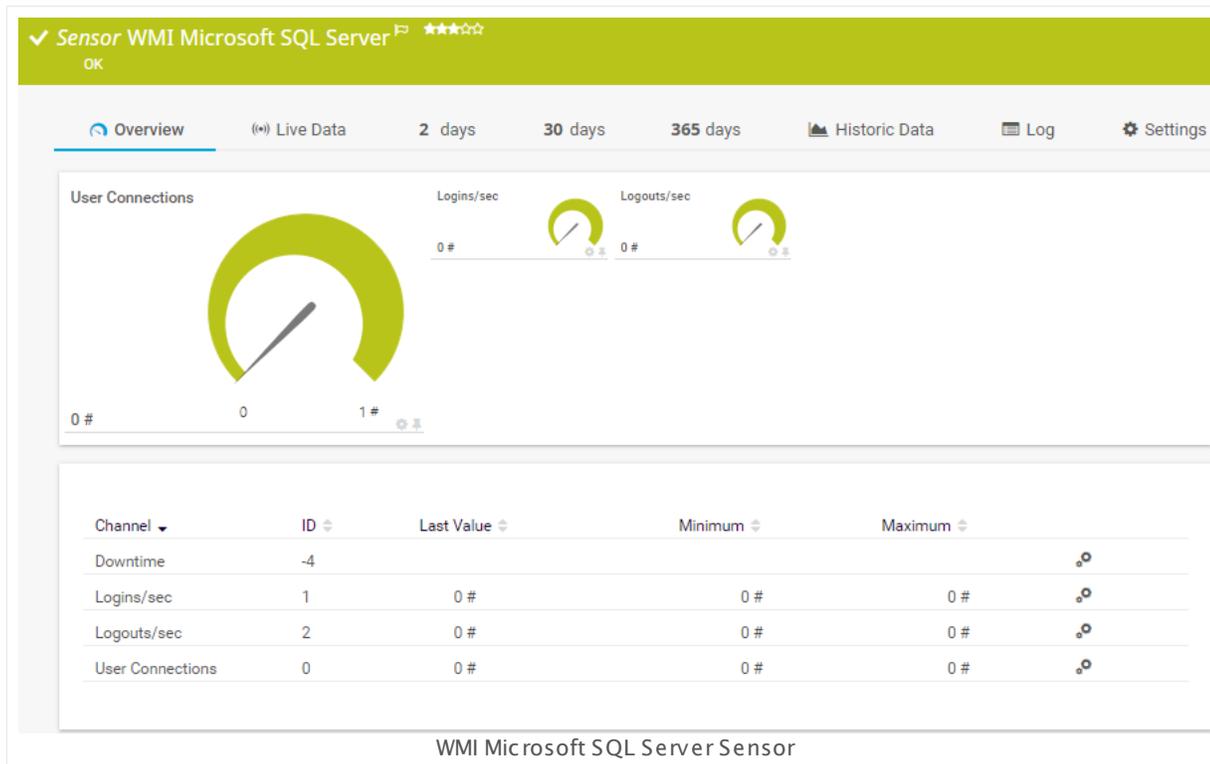
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

243 WMI Microsoft SQL Server 2014 Sensor



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	<p>Enter the version of the SQL Server. Usually, you can keep the default value.</p>

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none">▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.▪ Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).▪ Buffer Manager: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.▪ Memory Manager: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).▪ Locks: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.▪ SQL Statistics: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).
--------------------------	---

SQL COUNTER SPECIFIC

Depending on your selection, PRTG creates a sensor with the specified channels.

- ⓘ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Class Name Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:

- **Automatic:** Choose WMI class automatically. We recommend this setting.
- **Manual:** Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.

WMI Class This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SQL SERVER SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

SQL Performance Counters Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.244 WMI Microsoft SQL Server 2016 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

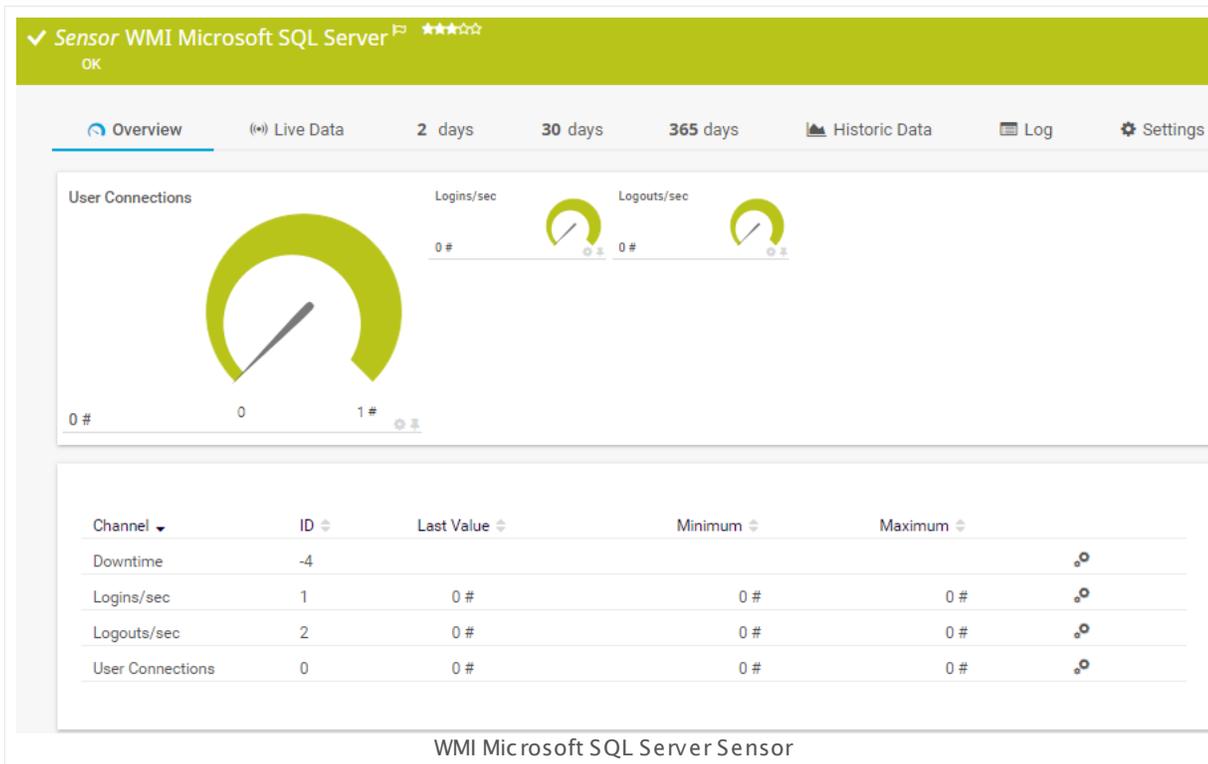
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

244 WMI Microsoft SQL Server 2016 Sensor



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	<p>Enter the version of the SQL Server. Usually, you can keep the default value.</p>

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none">▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.▪ Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).▪ Buffer Manager: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.▪ Memory Manager: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).▪ Locks: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.▪ SQL Statistics: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).
--------------------------	---

SQL COUNTER SPECIFIC

Depending on your selection, PRTG creates a sensor with the specified channels.

- ⓘ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Class Name Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:

- **Automatic:** Choose WMI class automatically. We recommend this setting.
- **Manual:** Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.

WMI Class This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SQL SERVER SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

SQL Performance Counters Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule	<p>Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the account settings.</p> <ul style="list-style-type: none"> <p>i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.</p>
Maintenance Window	<p>Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:</p> <ul style="list-style-type: none"> <p>▪ Not set (monitor continuously): No maintenance window will be set and monitoring will always be active.</p> <p>▪ Set up a one-time maintenance window: Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.</p> <ul style="list-style-type: none"> <p>i To terminate a current maintenance window before the defined end date, change the time entry in Maintenance Ends field to a date in the past.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.245 WMI Microsoft SQL Server 2017 Sensor

The WMI Microsoft SQL Server sensor monitors the performance of a Microsoft SQL Server via Windows Management Instrumentation (WMI). This sensor can monitor **SQL General Statistics**, **Access Methods**, the **Buffer Manager**, the **Memory Manager**, the **Locks Manager**, and **SQL Statistics**. The channels that are actually available for a sensor depend on the performance counters that you choose during setup.

CHANNEL OVERVIEW

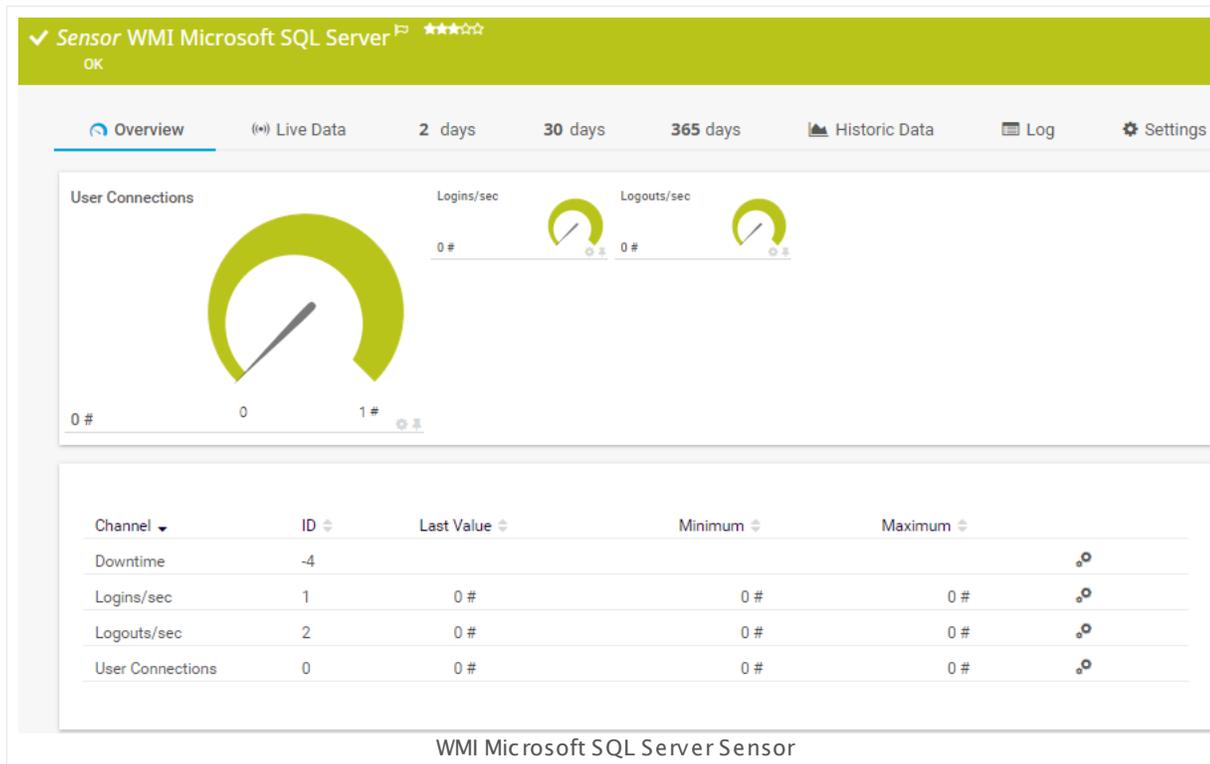
User Connections	Number of user connections. Because each user connection consumes some memory, configuring overly high numbers of user connections could affect throughput. Set user connections to the maximum expected number of concurrent users.
Logins	Total number of logins started per second.
Logouts	Total number of logout operations started per second.
Full Scans	Number of unrestricted full scans per second. These can be either base-table or full-index scans.
Page Splits	Number of page splits per second that occur as the result of overflowing index pages.
Table Lock Escalations	Number of times locks on a table were escalated.
Buffer Cache Hit Ratio	<p>Percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started. After a long period of time, the ratio moves very little.</p> <p>Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server.</p>
Database Pages	Number of pages in the buffer pool with database content.
Stolen Pages	Number of pages used for miscellaneous server purposes (including procedure cache).
Page Life Expectancy	Number of seconds a page will stay in the buffer pool without references.
Connection Memory (KB)	Total amount of dynamic memory the server is using for maintaining connections.

CHANNEL OVERVIEW

Optimizer Memory (KB)	Total amount of dynamic memory the server is using for query optimization.
Total Server Memory (KB)	Total amount of dynamic memory (in kilobytes) that the server is using currently.
Target Server Memory (KB)	Total amount of dynamic memory the server can consume.
SQL Cache Memory (KB)	Total amount of dynamic memory the server is using for the dynamic SQL cache.
Lock Requests	Number of new locks and lock conversions per second requested from the lock manager.
Deadlocks	Number of lock requests per second that resulted in a deadlock.
Average Wait Time	Average amount of wait time (in milliseconds) for each lock request that resulted in a wait.
Batch Requests	Number of Transact-SQL command batches received per second. This statistic is affected by all constraints (such as I/O, number of users, cache size, complexity of requests, and so on). High batch requests mean good throughput.
SQL Compilations	Number of SQL compilations per second. Indicates the number of times the compile code path is entered. Includes compiles due to recompiles. After SQL Server user activity is stable, this value reaches a steady state.
SQL Re-Compilations	Number of SQL recompiles per second. Counts the number of times recompiles are triggered. In general, you want the recompiles to be low.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings

245 WMI Microsoft SQL Server 2017 Sensor



Remarks

- This sensor can only be added to a device (computer) running a Microsoft SQL database.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

☁ You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the instances of the Microsoft SQL Server you want to monitor. PRTG will create one sensor for each instance you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

SQL SERVER SETTINGS

MS SQL Server Instance	<p>You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.</p> <p> Display name and service name are provided as returned by the SQL Server.</p>
SQL Server Version	<p>Enter the version of the SQL Server. Usually, you can keep the default value.</p>

SQL COUNTER SPECIFIC

SQL Performance Counters	<p>You see a list of different groups of performance counters that the sensor can monitor for the instance(s) that you selected above. Every sensor that PRTG creates for the server instances monitors the performance counters you select here. Choose from:</p> <ul style="list-style-type: none">▪ General Statistics: Read general performance counters. This shows the number of user connections, and the number of logins and logouts per second.▪ Access Methods: Read access method counters. This shows the number of full scans, page splits, and table lock escalations (per second).▪ Buffer Manager: Read buffer manager counters. This shows the buffer cache hit ratio in percent, and the number of database pages and stolen pages.▪ Memory Manager: Read memory manager counters. This shows the connection memory, optimizer memory, total server memory, target server memory, and SQL cache memory (in kb).▪ Locks: Read locks counters. This shows the number of lock requests and deadlocks (per second), and the average wait time.▪ SQL Statistics: Read SQL statistics. This shows the number of batch requests, SQL compilations, and SQL re-compilations (per second).
--------------------------	---

SQL COUNTER SPECIFIC

Depending on your selection, PRTG creates a sensor with the specified channels.

- ⓘ To monitor more than one of the listed groups of performance counters, please add the sensor several times for the instance (s).

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

- ⓘ Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <ul style="list-style-type: none"> ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SQL SERVER SETTINGS

Service Shows the service that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Name Shows the name of the server instance that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI Class Name Select whether PRTG selects the name of the WMI class used for monitoring automatically. Choose between:

- **Automatic:** Choose WMI class automatically. We recommend this setting.
- **Manual:** Manually enter a WMI class name. Select this option if your server instance returns an error code in automatic mode.

WMI Class This field is only visible if you enable manual WMI class selection above. This setting is intended for experienced users only. Enter the WMI class name that the sensor uses for monitoring your server instance.

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

SQL SERVER SETTINGS

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SQL COUNTER SPECIFIC

SQL Performance Counters Shows the performance counter that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

SENSOR DISPLAY

Primary Channel Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

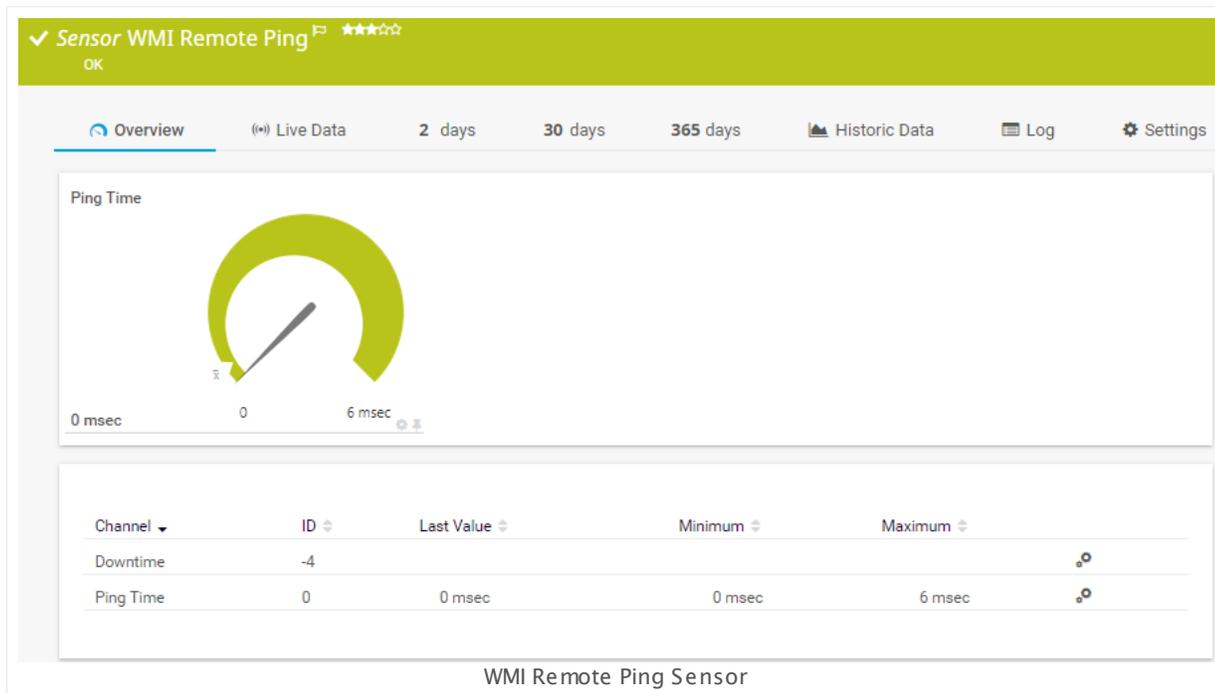
Others

For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.246 WMI Remote Ping Sensor

The WMI Remote Ping sensor remotely connects to a Windows system using Windows Management Instrumentation (WMI) and performs an Internet Control Message Protocol (ICMP) echo request ("Ping") from this device to a specified target.

- The sensor shows the Ping time from the remote device to the target device that is being pinged.



Sensor in Other Languages

Dutch: **WMI Remote Ping**, French: **Ping distant WMI**, German: **WMI Remote Ping**, Japanese: **WMI ? ? ? ? P I N G ? ?**, Portuguese: **Ping remoto de WMI**, Russian: **Удаленная проверка связи WMI**, Simplified Chinese: **WMI ? ? Ping**, Spanish: **Ping remoto WMI**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI REMOTE PING CONFIGURATION

Target	Enter the DNS name or IP address of the target device to send the ping to. The sensor remotely connects to its parent device via WMI. Then it performs a ping request from this remote device to the target device or server. Please enter a string.
Timeout (Sec.)	Enter a timeout in seconds for the Ping. If the reply takes longer than this value defines, the sensor cancels the request and triggers an error message. Please enter an integer value. The maximum timeout value is 300 .
Packet Size (Bytes)	Enter the packet size in bytes for the Ping. You can use any value between 1 and 10000 . Please enter an integer value. We recommend that you use the default value.

DEBUG OPTIONS

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none">▪ Discard sensor result: Do not store the sensor result.▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval.  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
246 WMI Remote Ping Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.247 WMI Security Center Sensor

The WMI Security Center sensor monitors the security status of a Windows client computer using Windows Management Instrumentation (WMI). It can monitor all security products that are controlled by Windows Security Center / Windows Action Center.

- It shows the status code of the monitored product and sets the sensor status accordingly. A [sensor status](#) showing **Up** indicates that the product is up to date and the access scan is running.

Possible return values for status codes are:

Status Code	Meaning: Status of Monitored Security Product Is ...	Will Result in Sensor Status
0	Unknown	Down
1	Not running, Out of date	Down
2	Running, Out of date	Warning
3	Not running, Up to date	Down
4	Running, Up to date	OK

✓ Sensor WMI Security Center ☆☆☆☆
OK

Overview
Live Data
2 days
30 days
365 days
Historic Data
Log
Settings

Status



Running - Up to Date

Channel	ID	Last Value	Minimum	Maximum	
Downtime	-4				⚙️
Status	0	Running - Up to Date	Running - Up to Date	Running - Up to Date	⚙️

WMI Security Center Sensor

Sensor in Other Languages

Dutch: **WMI Security Center**, French: **Centre de sécurité WMI**, German: **WMI Sicherheits-Center**, Japanese: **WMI** ? ? ? ? ? ? ? ? ? ? , Portuguese: **Centro de segurança WMI**, Russian: **Центр безопасности WMI**, Simplified Chinese: **WMI** ? ? ? ? , Spanish: **Centro de seguridad WMI**

Remarks

- This sensor requires Windows Vista or later on the target computer.
- This sensor type does not run on Windows Server operating systems (Windows Server 2003, 2008, 2012, 2016), because the Windows Security Center / Windows Action Center is only available on client Windows versions.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)¹²⁵. Above this number, please consider using multiple [Remote Probes](#)³⁷⁰⁹ for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)³⁵⁰⁷.
- This sensor type uses lookups to determine the status values of one or more sensor channels. This means that possible states are defined in a lookup file. You can change the behavior of a channel by editing the lookup file that this channel uses. For details, see the manual section [Define Lookups](#)³⁶⁹³.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the security center products you want to monitor. PRTG will create one sensor for each product you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SECURITY CENTER SPECIFIC

Security Center Products You see a list showing the **Name** and **Type** of all security products found in the Windows Security Center on the target device. If there are no products, you see a corresponding message.

Add check marks in front of the respective lines to select the desired items. PRTG will create one sensor for each selection. You can also select and deselect all items by using the check box in the table head.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the [device tree](#), as well as in [alarms](#), [logs](#), [notifications](#), [reports](#), [maps](#), [libraries](#), and [tickets](#).

Parent Tags Shows [Tags](#) that this sensor [inherits](#) from its [parent device, group, and probe](#). This setting is shown for your information only and cannot be changed here.

Tags Enter one or more [Tags](#), separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#) from objects further up in the device tree. These are visible above as **Parent Tags**.

i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

BASIC SENSOR SETTINGS

Priority Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SECURITY CENTER SPECIFIC

Display Name Shows the name of the product monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Type Shows the type of the product monitored by this sensor. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

DEBUG OPTIONS

Sensor Result Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 - 🔗 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <p> This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).</p>
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁵ on PRTG on premises installations.</p>
-------------------	--

SCANNING INTERVAL

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#) 3311.

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Select object**: Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent**: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[329] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency

This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay
(Sec.)

Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
247 WMI Security Center Sensor

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.248 WMI Service Sensor

The WMI Service sensor monitors a Windows service using Windows Management Instrumentation (WMI).

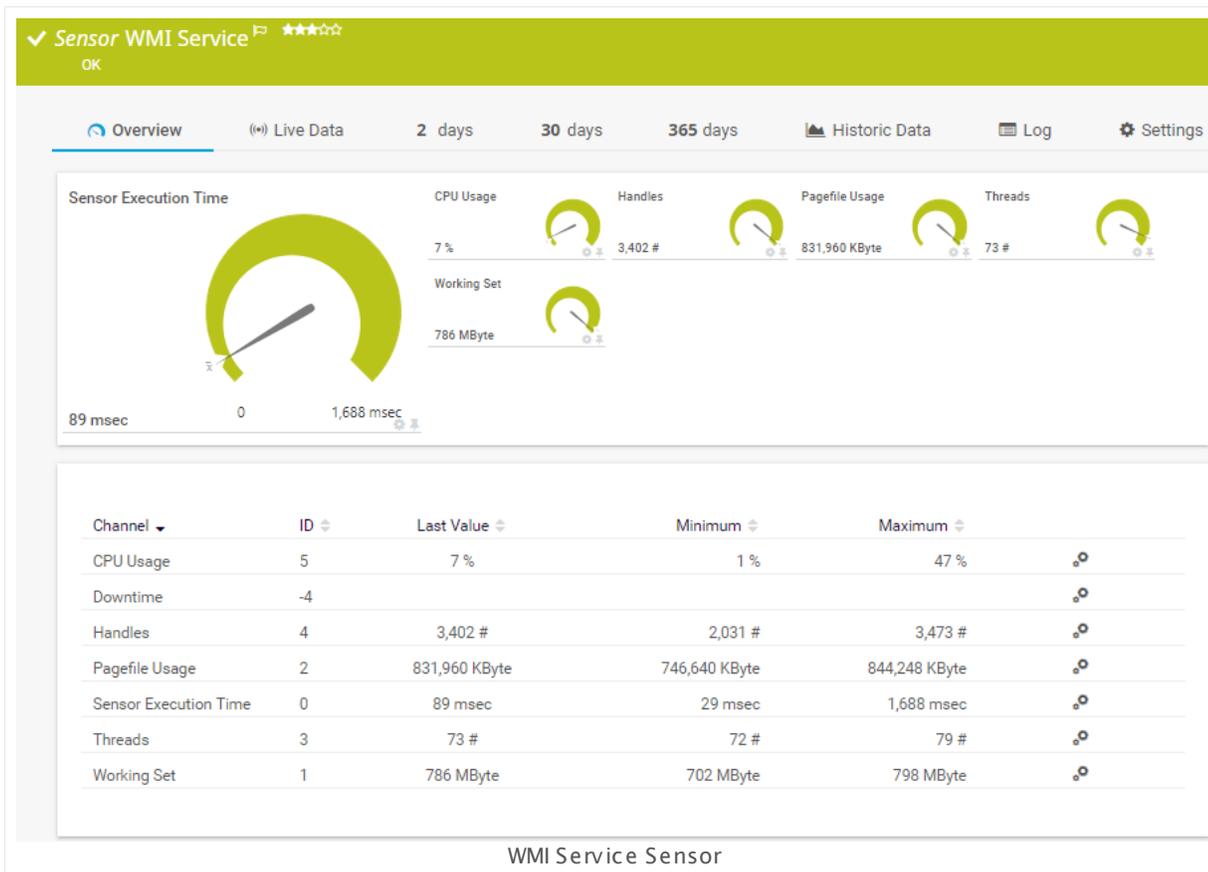
It can show the following:

- Execution time of the monitoring request.

Additionally, if you enable **Monitor extended values** in the sensor settings, it can show these parameters:

- CPU usage in percent
- Pagefile usage in bytes
- Number of handles
- Number of threads
- Working set in bytes

i The "Running (msec)" channel of this sensor shows the execution time of the monitoring request. It does **not** refer to the time the Windows service has been running! As of PRTG version 13, the name of this sensor channel is **Sensor Execution Time**.



Sensor in Other Languages

Dutch: **WMI Service**, French: **Service WMI**, German: **WMI Dienst**, Japanese: **WMI ? ? ? ?**, Portuguese: **Serviço WMI**, Russian: **Служба WMI**, Simplified Chinese: **WMI ? ?**, Spanish: **WMI servicio**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
 - Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
 - For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the Windows services you want to monitor. PRTG will create one sensor for each service you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SERVICE MONITOR

Service

You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items. Name and description are provided in the language of the device's Windows installation.

-  Once set up, the sensor will show a **Down status**^[195] if the service is not running.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SERVICE MONITOR

If Service is Not Running	Select whether you want PRTG to (re)start the service if it is stopped or paused. Choose between:
---------------------------	---

WMI SERVICE MONITOR

- **Start/Restart service:** PRTG tries to start the service if it is not running when scanning the device. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³¹⁷⁰ whenever PRTG (re)starts the service.

- **Do nothing:** PRTG will not start any service on the device automatically.

i If you select the start/restart option and the sensor detects that the monitored service does not run, PRTG will try to restart the service during this scan and postpones the next sensor scan for one interval. With this following scan, the sensor will check if the service now is running. If starting the service was not successful or the service failed again, the sensor will show a **Down status**¹⁹⁵ and not try to start the service again. If the service runs after a (re)start attempt, the sensor will continue monitoring as usual.

If Service is Restarted

This setting is only visible if you select **Start/Restart service** above. Define what to do if PRTG restarts the service. Choose between:

- **Ignore changes:** No action is taken on change.
- **Trigger 'change' notification:** The sensor will send an internal message indicating that its value has changed. In combination with a **Change Trigger**, you can use this mechanism to [trigger a notification](#)³¹⁷⁰ whenever the sensor value changes.

Monitoring

Select whether you want to monitor CPU usage and other useful performance counters. Choose between:

- **Just check if service is running:** PRTG only monitors the channel **Sensor Execution Time**.
 - **Monitor extended values:** PRTG also monitors other useful performance counters.
- i** Extended monitoring might cause a **Class not found** error on some Windows systems.

Service

Shows the Windows service this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

Description

Shows the description of the service. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.

WMI SERVICE MONITOR

- Sensor Result** Define what PRTG will do with the sensor results. Choose between:
- **Discard sensor result:** Do not store the sensor result.
 - **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

- Primary Channel** Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.
-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.
- Graph Type** Define how different channels will be shown for this sensor.
- **Show channels independently (default):** Show an own graph for each channel.
 - **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).
- Stack Unit** This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

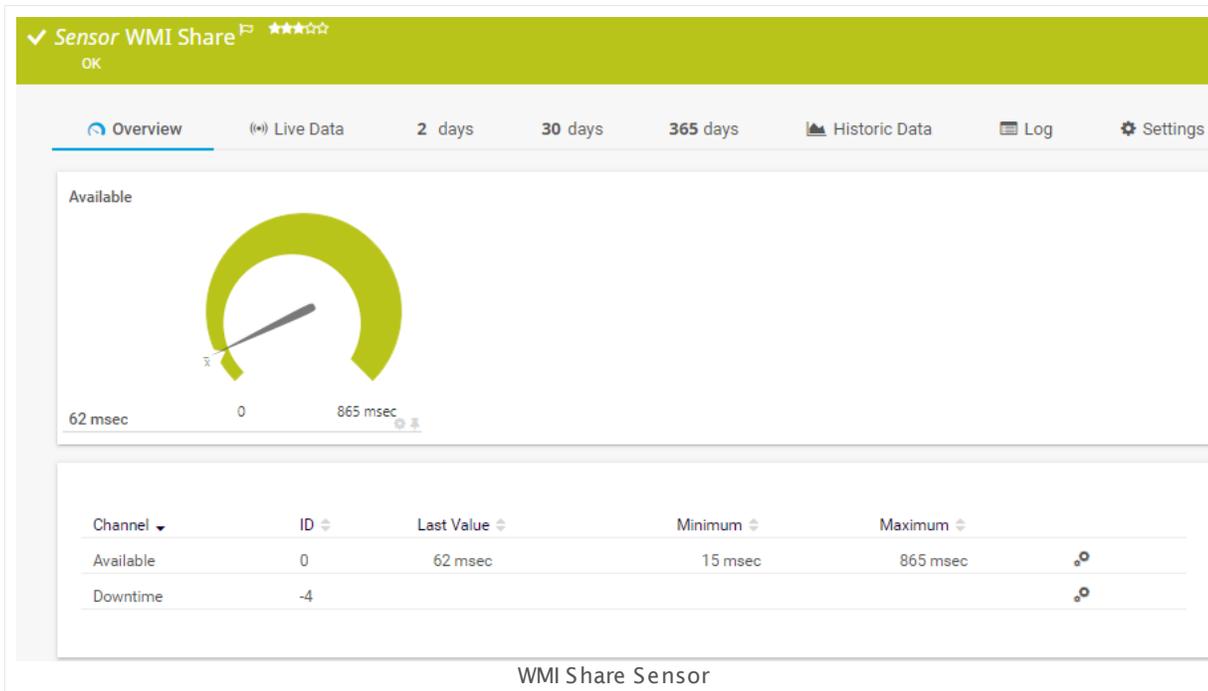
For more general information about settings, see the [Object Settings](#)²¹⁷ section.

7.8.249 WMI Share Sensor

The WMI Share sensor monitors a shared resource on a Windows system using Windows Management Instrumentation (WMI).

- It shows the availability of the share.

You can define the sensor to show a **Down status** for different share status messages.



Sensor in Other Languages

Dutch: **WMI Share**, French: **Partage WMI**, German: **WMI Freigabe**, Japanese: **WMI ? ?**,
Portuguese: **Compartilhamento WMI**, Russian: **Ресурс WMI**, Simplified Chinese: **WMI ? ?**,
Spanish: **Recurso compartido WMI**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per **probe**. Above this number, please consider using multiple **Remote Probes** for load balancing.
- For a general introduction to the technology behind WMI, please see manual section **Monitoring via WMI**.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the shares you want to monitor. PRTG will create one sensor for each share you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI SHARED RESOURCE

Share	Select the shares you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
	 To provide any shares, the LanmanServer "Server" Windows service must be running on the target computer. If it is not, there are no shares and you see a No Share available message here.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI SHARED RESOURCE

Shared Resource	
Description	Shows information about the shared resource that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Type	
TypeID	

TRIGGER ERROR STATE ON FOLLOWING CONDITIONS

Select under which conditions the sensor shows a **Down status** from the list below. As long as the share returns OK, the sensor status is **Up**. Add a check mark symbol in front of the according line to choose a **Down** condition. Choose none, one, or several of the following conditions.

While in Down status, a sensor does not record any data in any of its channels.

Error	Set sensor to Down status if the share returns an error status. A share in this status is not operational. This condition is selected by default.
Degraded	Set sensor to Down status if the share returns a degraded status. A share in this status is still operational. This condition is selected by default.
Unknown	Set sensor to Down status if the share returns an unknown status.
Pred Fail	Set sensor to Down status if the share returns a "predicted fail" status. This indicates that an element works properly but predicts a failure (for example, a SMART-enabled hard drive). A share in this status is still operational. This condition is selected by default.
Starting	Set sensor to Down status if the share returns a starting status. A share in this status is not operational.
Stopping	Set sensor to Down status if the share returns a stopping status. A share in this status is not operational.
Service	Set sensor to Down status if the share returns a service status. This can apply during disk mirror-resilvering, reloading a user permissions list, or other administrative work on the monitored device. Not all such work is online, but the managed element is neither OK nor in one of the other states. A share in this status is not operational.
Stressed	Set sensor to Down status if the share returns a stressed status.
Nonrecover	Set sensor to Down status if the share returns a "non recover" status. This condition is selected by default.
NoContact	Set sensor to Down status if the share returns a "no contact" status. This condition is selected by default.
LostComm	Set sensor to Down status if the share returns "lost communication" status. This condition is selected by default.

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.
- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

i Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#) 3209 in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

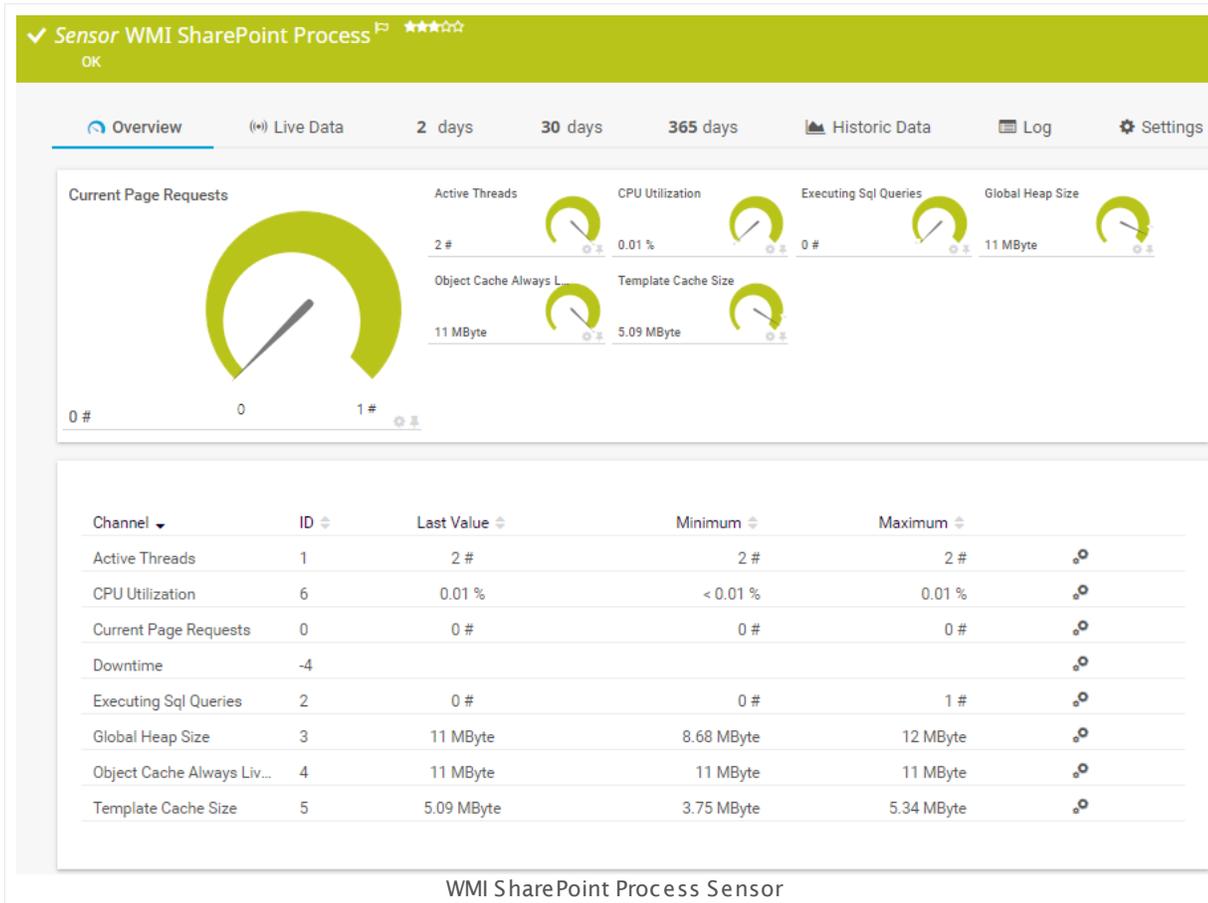
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.250 WMI SharePoint Process Sensor

The WMI SharePoint Process sensor monitors a Microsoft SharePoint server using Windows Management Instrumentation (WMI).

It can show the following:

- Number of current page requests
- Number of active threads
- Number of currently executed SQL queries
- Global heap size
- Object cache always live size
- Template cache size
- CPU utilization in percent



Sensor in Other Languages

Dutch: **WMI SharePoint Proces**, French: **Processus WMI SharePoint**, German: **WMI SharePoint-Prozess**, Japanese: **WMI SharePoint** ? ? ? ? , Portuguese: **Processo WMI SharePoint**,

Russian: **Процесс SharePoint WMI**, Simplified Chinese: WMI Sharepoint ? ? , Spanish: **WMI proceso SharePoint**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the SharePoint processes you want to monitor. PRTG will create one sensor for each process you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI PROCESS MONITOR

SharePoint Processes	You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
----------------------	--

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI PROCESS MONITOR

SharePoint Process	Shows the name of the SharePoint process that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
--------------------	--

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.

 This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.251 WMI Terminal Services (Windows 2008+) Sensor

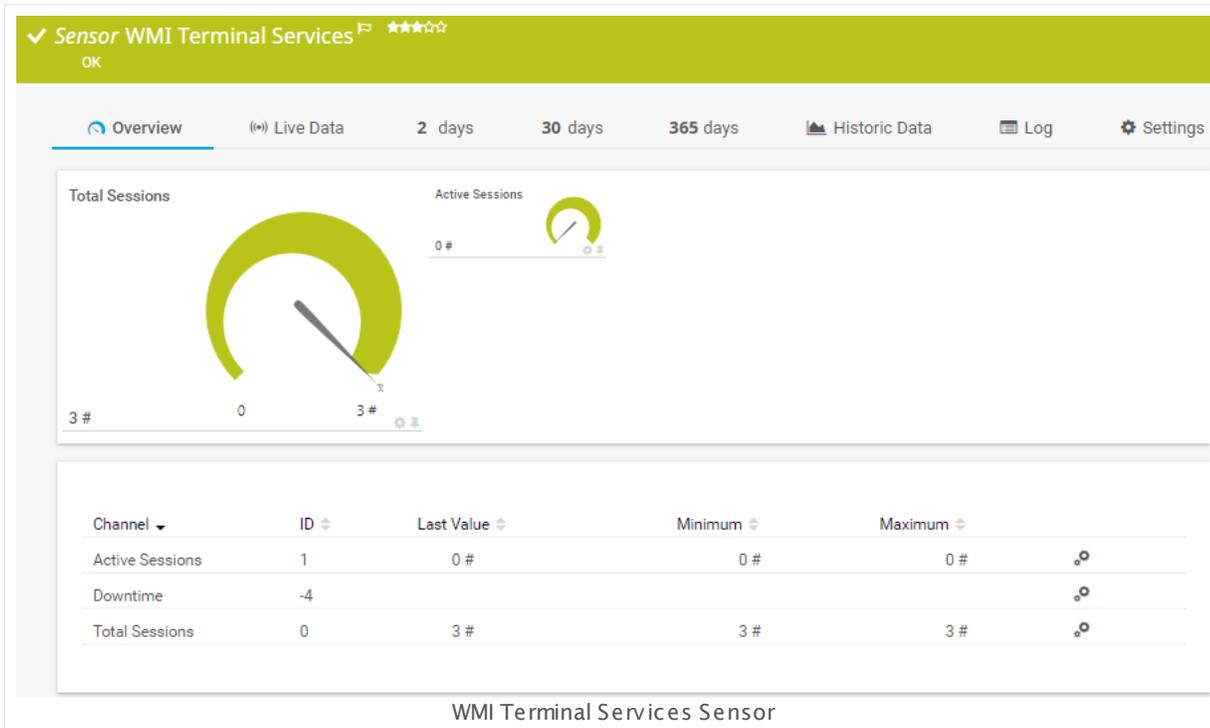
Sensor in Other Languages

Dutch: **WMI Terminal Services (Win2008+)**, French: **Services Terminal WMI (Win2008++)**, German: **WMI Terminaldienst e (Windows 2008+)**, Japanese: **WMI ? ? ? ? ? ? ? ? ?** (**W I ndows 2008+**) , Portuguese: **Serviços de terminal WMI (Win2008+)**, Russian: **WMI служб терминалов (Win2008 и последующая)**, Simplified Chinese: **WMI ? ? ? ? (Win2008+)**, Spanish: **WMI Terminal Services (Win2008+)**

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI).

It shows the following:

- Number of active sessions: sessions with a currently logged in user, including used published applications
- Number total sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out, or system services using a session



Remarks

- For the **Total Sessions** channel, the sensor returns the number of active and inactive sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.
- Depending on the OS that you want to monitor, select either the sensor for Windows XP/ Vista/2003 or the one for Windows 2008 R2 and later.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings^[3160] settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)^[331] group's settings, see section [Inheritance of Settings](#)^[137] for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration^[336] on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status^[195]. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.252 WMI Terminal Services (Windows XP/Vista/2003) Sensor

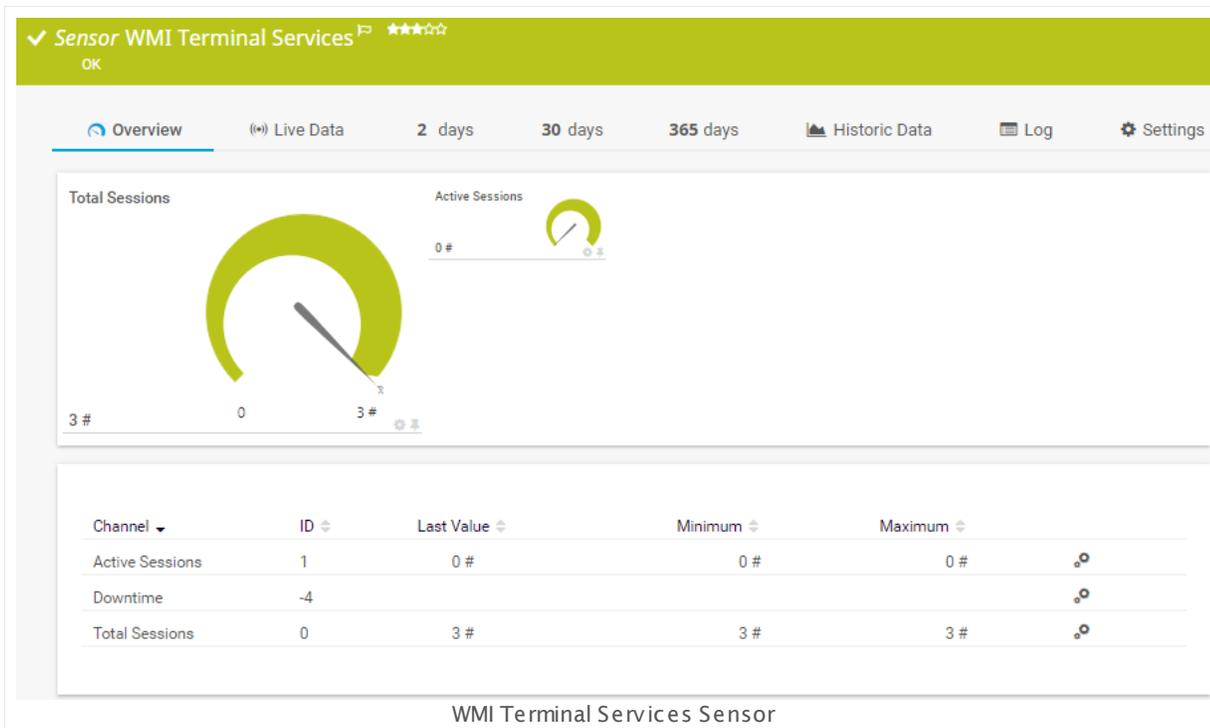
Sensor in Other Languages

Dutch: **WMI Terminal Services XP/Vista/2k3**, French: **Services Terminal WMI XP/Vista/2k3**, German: **WMI Terminaldienst (XP/Vista/2003)**, Japanese: **WMI ? ? ? ? ? ? ? ? ? (XP/VI sta/2003)** , Portuguese: **Serviços de terminal do WMI XP/Vista/2k3**, Russian: **WMI служб терминалов XP/Vista/2k3**, Simplified Chinese: **WMI ? ? ? ? XP/Vista/2k3**, Spanish: **WMI Terminal Services XP/Vista/2k3**

The WMI Terminal Services sensor monitors the number of sessions on a Windows Terminal Services (Remote Desktop Services) server using Windows Management Instrumentation (WMI).

It shows the following:

- Number of active sessions: sessions with a currently logged in user, including used published applications
- Number total sessions (including inactive sessions): inactive sessions can be sessions with a disconnected user that has not logged out, or system services using a session



Remarks

- For the **Total Sessions** channel, the sensor returns the number of active and inactive sessions, plus two additional sessions: one for the console, and another for the services. So, the number of total sessions may actually be higher than expected.
- Depending on the OS that you want to monitor, select either the sensor for Windows XP/Vista/2003 or the one for Windows 2008 R2 and later.

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3276] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	Enter one or more Tags ^[139] , separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.

BASIC SENSOR SETTINGS

You can add additional tags to the sensor if you like. Other tags are automatically [inherited](#)¹⁴⁰¹ from objects further up in the device tree. These are visible above as **Parent Tags**.

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Priority

Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result**: Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt")**: Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

SENSOR DISPLAY

Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none"> ⓘ This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval	<p>Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration³³⁶ on PRTG on premises installations.</p>
If a Sensor Query Fails	<p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p>

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Part 7: Ajax Web Interface—Device and Sensor Setup | 8 Sensor Settings
252 WMI Terminal Services (Windows XP/Vista/2003) Sensor

Others

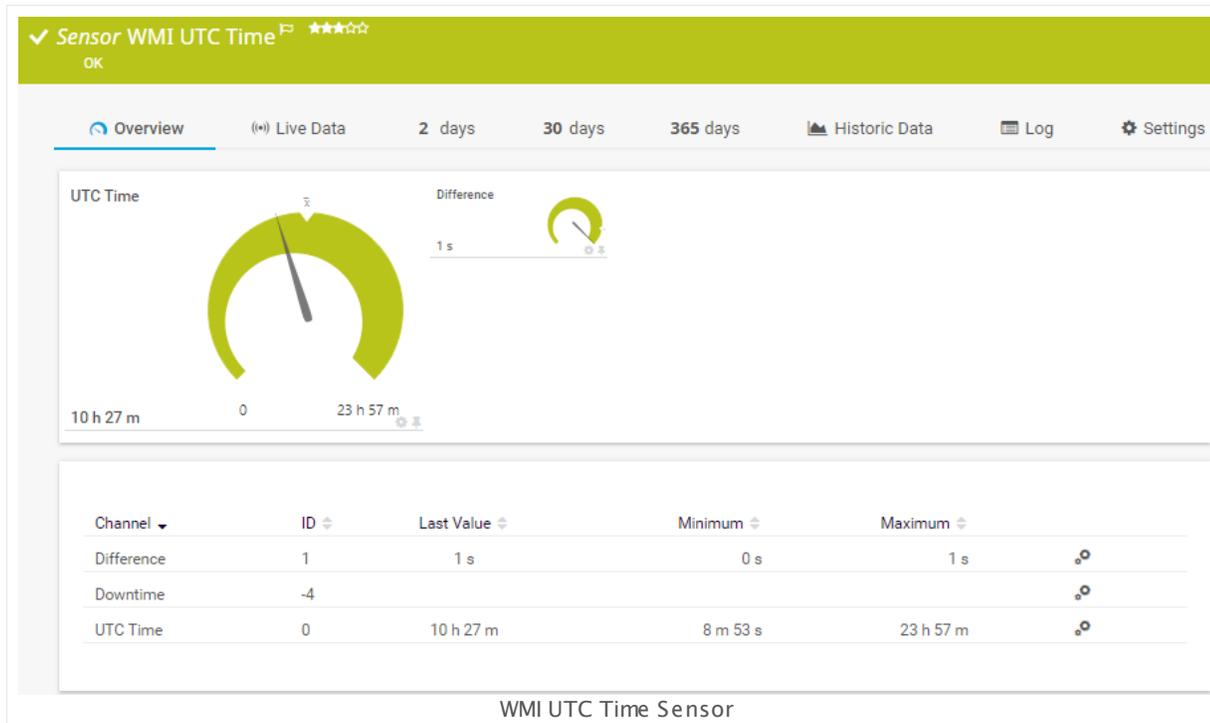
For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.253 WMI UTC Time Sensor

The WMI UTC Time sensor monitors the UTC (Coordinated Universal Time) time of a target device using Windows Management Instrumentation (WMI).

It shows the following:

- UTC time of the target device
- Time difference between the PRTG system time and the target device in seconds



Sensor in Other Languages

Dutch: **WMI UTC Tijd**, French: **Heure UTC WMI**, German: **WMI UTC-Zeit**, Japanese: **WMI UTC ? ?**, Portuguese: **Tempo UTC de WMI**, Russian: **Время WMI UTC**, Simplified Chinese: **WMI UTC ? ?**, Spanish: **WMI tiempo UTC**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
- Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
- For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#) add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#) for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.
 -  For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.
 -  This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 -  This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

SENSOR DISPLAY

Stack Unit This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.

SCANNING INTERVAL

- **Set sensor to "warning" for 3 intervals, then set to "down":**
Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":**
Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":**
Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
 - **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p>i Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies <small>3209</small> in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ^[240] to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	<p>Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.</p> <p> This setting is not available if you choose this sensor to Use parent or to be the Master object for parent. In this case, please define delays in the parent Device Settings^[402] or in the superior Group Settings^[375].</p>

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)³¹⁶⁰ section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)³¹⁷⁰ section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

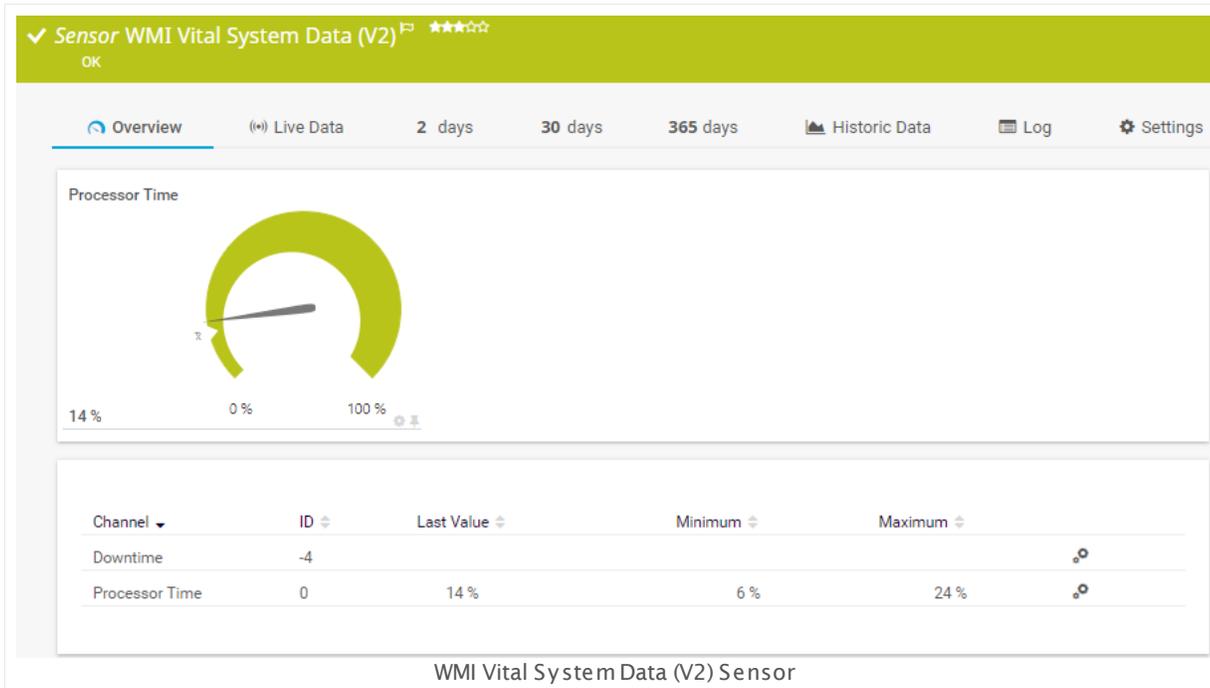
7.8.254 WMI Vital System Data (V2) Sensor

The WMI Vital System Data sensor monitors vital system parameters (CPU, thread, memory, network, pagefile) using Windows Management Instrumentation (WMI).

It can show the following:

- CPU usage: Processor, privileged, and user time
- CPU queue length
- Thread context switches
- Free physical memory
- Total visible memory
- Memory page faults, reads, and writes per second
- Memory pool paged and nonpaged bytes
- Memory committed bytes
- Network sent, received, and total bytes per second
- Network packets outbound errors
- Pagefile usage in percent
- Physical disk time in percent
- Current physical disk queue length
- Physical disk reads and writes per second
- Server bytes received, transmitted, and total
- CLR memory bytes in all heaps
- Thrown CLR exceptions per second

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **WMI Vitale Systeem Gegevens (V2)**, French: **Données importantes du syst. WMI (V2)**, German: **WMI Wichtige Systemdaten (v2)**, Japanese: **WMI ? ? ? ? ? ? ? ? ? ? (V2)**, Portuguese: **Dados vitais do sistema de WMI (V2)**, Russian: **Важные системные данные WMI (V2)**, Simplified Chinese: **WMI ? ? ? ? ? (V2)**, Spanish: **WMI Datos vitales de sistema (V2)**

Remarks

- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.
 - WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
 - Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
 - For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)³²⁵ add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the performance counters you want to monitor. PRTG will create one sensor for each counter you select in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

VITAL SYSTEM DATA READINGS ACCESSIBLE USING WMI

Performance Counter You see a list of available vital system data values the sensor can monitor on the target device. The available options depend on your configuration. PRTG shows all possible performance counters with name and instance description (if available).

Add check marks in front of the respective lines to select the desired items. PRTG will create one sensor for each selection. You can also select and deselect all items by using the check box in the table head.

You can choose between the following counters:

- CPU
- Thread
- Memory
- Network
- Pagefile

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)⁴⁰² for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

READINGS ACCESSIBLE USING WMI

Display Name	These fields show the parameters that are used to query data for this sensor from the target device. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Instance	
WMI Class	
Counter	
Time Stamp	
Time Frequency	
Counter Type	

READINGS ACCESSIBLE USING WMI

Sensor Result	<p>Define what PRTG will do with the sensor results. Choose between:</p> <ul style="list-style-type: none"> ▪ Discard sensor result: Do not store the sensor result. ▪ Write sensor result to disk (Filename: "Result of Sensor [ID].txt"): Store the last result received from the sensor to the Logs (Sensor) directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This is for debugging purposes. PRTG overrides these files with each scanning interval. <ul style="list-style-type: none">  For more information on how to find the folder used for storage, see section Data Storage³⁷³⁴. <p> This option is not available when the sensor runs on the Hosted Probe of a PRTG hosted by Paessler instance.</p>
---------------	---

SENSOR DISPLAY

Primary Channel	<p>Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.</p> <p> You can set another primary channel later by clicking the pin symbol of a channel in the sensor's Overview tab.</p>
Graph Type	<p>Define how different channels will be shown for this sensor.</p> <ul style="list-style-type: none"> ▪ Show channels independently (default): Show an own graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic. <ul style="list-style-type: none">  This option cannot be used in combination with manual Vertical Axis Scaling (available in the Sensor Channels Settings³¹⁶⁰ settings).
Stack Unit	<p>This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.</p>

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#) group's settings, see section [Inheritance of Settings](#) for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#) for more information.

- | | |
|-------------------------|---|
| Scanning Interval | Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the system administration on PRTG on premises installations. |
| If a Sensor Query Fails | <p>Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a Down status. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a Warning status. Choose between:</p> <ul style="list-style-type: none">▪ Set sensor to "down" immediately: The sensor will show an error immediately after the first failed request.▪ Set sensor to "warning" for 1 interval, then set to "down" (recommended): After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.▪ Set sensor to "warning" for 2 intervals, then set to "down": Show an error status only after three consecutively failed requests.▪ Set sensor to "warning" for 3 intervals, then set to "down": Show an error status only after four consecutively failed requests.▪ Set sensor to "warning" for 4 intervals, then set to "down": Show an error status only after five consecutively failed requests.▪ Set sensor to "warning" for 5 intervals, then set to "down": Show an error status only after six consecutively failed requests. |

SCANNING INTERVAL

- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#) values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#).

- i** Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.
- i** To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

Maintenance Begins	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.
Maintenance Ends	This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.
Dependency Type	<p>Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:</p> <ul style="list-style-type: none"> ▪ Use parent: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. ▪ Select object: Pause the current sensor if the device, where it is created on, is in Down status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in Down status, or is paused by another dependency. Select below. ▪ Master object for parent: Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in Down status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in Down status, or if it is paused by another dependency. <p> Testing your dependencies is easy! Simply choose Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can check all dependencies³²⁰⁹ in your PRTG installation by selecting Devices Dependencies from the main menu bar.</p>
Dependency	This field is only visible if the Select object option is enabled above. Click on the reading-glasses and use the object selector ²⁴⁰ to choose an object on which the current sensor will depend.
Dependency Delay (Sec.)	Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to Up status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)⁴⁰² or in the superior [Group Settings](#)³⁷⁵.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

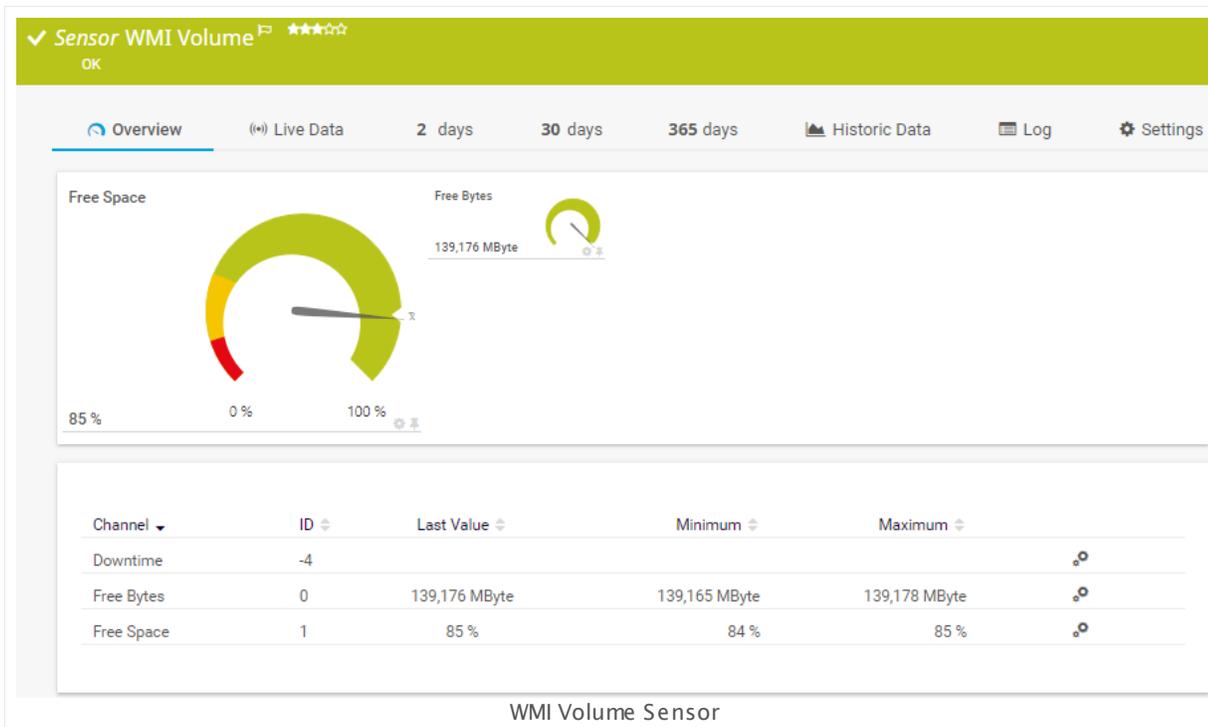
Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.8.255 WMI Volume Sensor

The WMI Volume sensor monitors the free disk space on a drive, logical volume, or mount point using Windows Management Instrumentation (WMI). For each drive, logical volume or mount point, PRTG will use one sensor.

- It shows free space in percent and total.
- ❗ The sensor monitors an area of storage on a hard disk. It can monitor local volumes that are formatted, unformatted, mounted, or offline. A volume is formatted by using a file system, such as File Allocation Table (FAT) or New Technology File System (NTFS), and might have a drive letter assigned to it. One hard disk can have multiple volumes, and volumes can span multiple physical disks.
- ❗ The sensor does not support disk drive management.



Sensor in Other Languages

Dutch: **WMI Volume**, French: **Disque WMI**, German: **WMI Datenträger**, Japanese: **WMI ? ? ?**, Portuguese: **Volume de WMI**, Russian: **Том WMI**, Simplified Chinese: **WMI ?**, Spanish: **WMI Volumen**

Remarks

- This sensor does not support Windows XP and earlier.
- Requires credentials for Windows systems to be defined for the device you want to use the sensor on.

- WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016.
 - Sensors using the Windows Management Instrumentation (WMI) protocol have high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[3709] for load balancing.
 - For a general introduction to the technology behind WMI, please see manual section [Monitoring via WMI](#)^[3507].
-  You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Select the volumes you want to monitor. PRTG will create one sensor for each volume you choose in the **Add Sensor** dialog. The settings you choose will be valid for all sensors that you create when you finish this dialog.

The following settings for this sensor differ in the Add Sensor dialog in comparison to the sensor's settings page.

WMI VOLUME SPECIFIC

Volumes	Select the volumes (drives, logical volumes, mount points) you want to add a sensor for. You see a list with the names of all items that are available to monitor. Add check marks in front of the respective lines to select the desired items. PRTG creates one sensor for each selection. You can also use the check box in the table head to select and deselect all items.
---------	---

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

 Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree , as well as in alarms , logs , notifications , reports , maps , libraries , and tickets .
Parent Tags	Shows Tags that this sensor inherits from its parent device, group, and probe . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags, separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited from objects further up in the device tree. These are visible above as Parent Tags.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

WMI VOLUME SPECIFIC

DeviceID	Shows the unique identifier of the volume that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
Drive Type	Shows the type of the disk drive that this sensor monitors. Once a sensor is created, you cannot change this value. It is shown for reference purposes only. If you need to change this, please add the sensor anew.
ID Selection	<p>Define how the sensor will identify the volume. Choose between:</p> <ul style="list-style-type: none"> ▪ Use system device ID (recommended): This is usually the best option for this sensor type, because the device ID will not change when the volume is renamed.

WMI VOLUME SPECIFIC

- **Use drive letter:** In a Microsoft cluster environment, the device ID will change when the cluster is switched to another node. In this case, use the drive letter option to avoid issues regarding this.

Drive Letter

This field is only visible if you select the drive letter option above. Enter the letter of the drive you want to monitor followed by a colon, for example, C:

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

- ☁ This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

-  You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

SENSOR DISPLAY

- **Show channels independently (default):** Show an own graph for each channel.
- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³¹ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

SCANNING INTERVAL

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.
 - **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
 - **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
 - **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
 - **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
 - **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.
- i** Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.
- i** If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.
- i** If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- i** Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can create new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

My WMI sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/1043>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

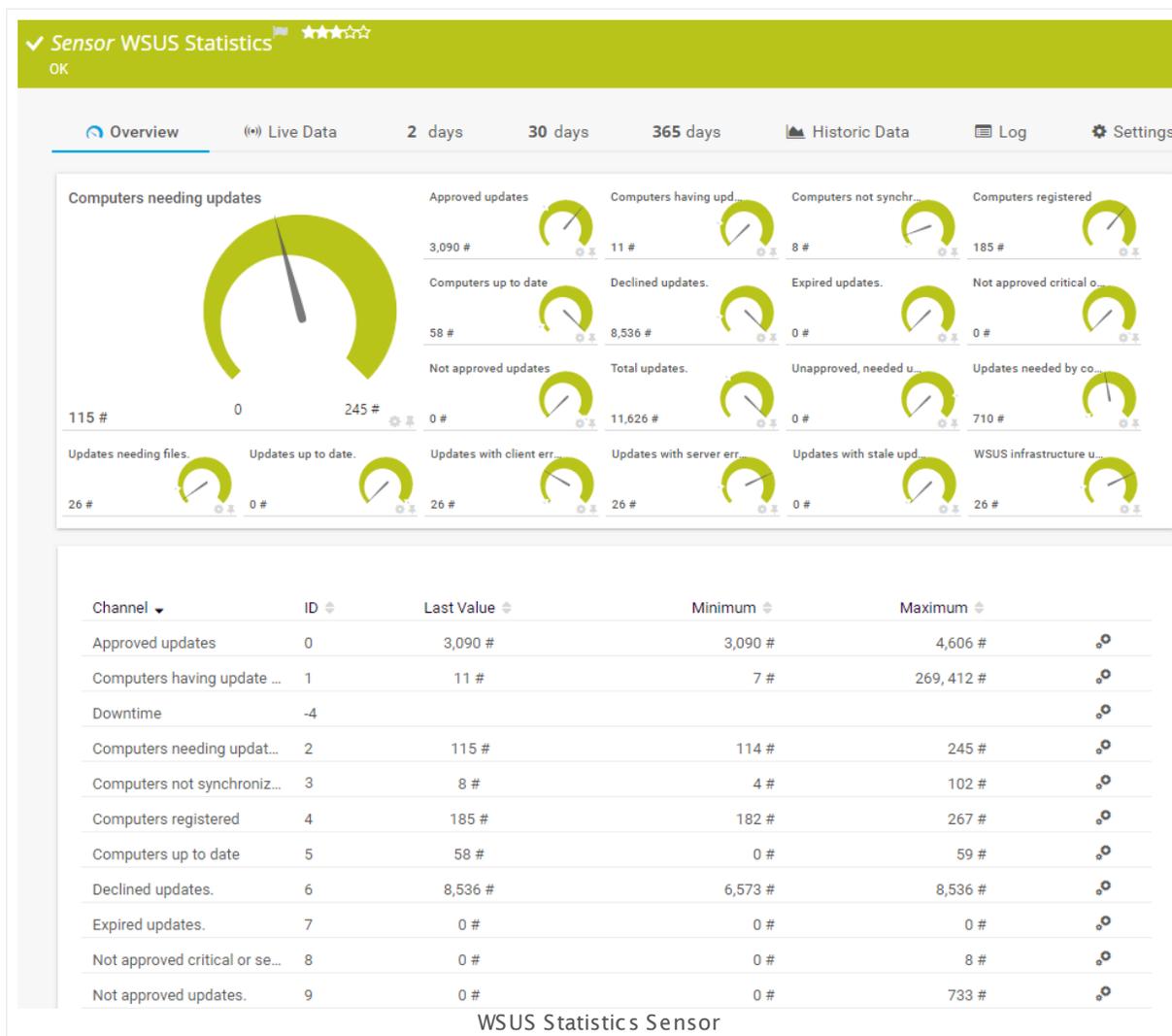
7.8.256 WSUS Statistics Sensor

The WSUS Statistics sensor monitors various statistics on a Windows Server Update Services (WSUS) server using Windows Management Instrumentation (WMI).

It can show the numbers of the following:

- Approved updates
- Computers having update errors
- Computers needing updates
- Computers not synchronized for 7 days
- Computers registered
- Computers up to date
- Declined updates
- Expired updates
- Not approved critical or security updates
- Not approved updates
- Total updates
- Unapproved needed updates
- Updates needed by computers
- Updates needing files
- Updates up to date
- Updates with client errors
- Updates with server errors
- Updates with stale update approvals
- Number of WSUS infrastructure updates not approved for installation

Which channels the sensor actually shows might depend on the monitored device and the sensor setup.



Sensor in Other Languages

Dutch: **WSUS Statistieken**, French: **Statistiques WSUS**, German: **WSUS-Statistiken**, Japanese: **WSUS ? ? ? ?**, Portuguese: **Estatísticas WSUS**, Russian: **Статистика WSUS**, Simplified Chinese: **WSUS ? ? ?**, Spanish: **Estadísticas WSUS**

Remarks

- [Requires](#) ^[3146] .NET 4.5 or later on the probe system. If the sensor shows the error PE087, please additionally install .NET 3.5 on the probe system.
- [Requires](#) ^[3146] WSUS 3.0 Administration Console on the probe system.
- [Requires](#) ^[3146] Windows credentials in the [parent device settings](#) ^[402].
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- Knowledge Base: [Can I encrypt connections to my WSUS server?](#)

- This sensor type can have a high impact on the performance of your monitoring system. Please use it with care! We recommend that you use no more than 50 sensors of this sensor type on each probe.

 You cannot add this sensor type to the **Hosted Probe** of a PRTG hosted by Paessler instance. If you want to use this sensor type, please add it to a remote probe device.

Requirement: .NET Framework

 This sensor type requires the **Microsoft .NET Framework** to be installed on the computer running the PRTG probe, either on the local system (on every node, if on a cluster probe), or on the system running the [remote probe](#)^[3709]. If the framework is missing, you cannot create this sensor.

Required **.NET** version (with latest update): .NET 4.5, .NET 4.6, or .NET 4.7.

 For more information, please see this Knowledge Base article: [Which .NET version does PRTG require?](#)

Requirement: Windows Credentials

Requires credentials for Windows systems to be defined for the device you want to use the sensor on. In the [parent device's](#)^[407] **Credentials for Windows Systems** settings, please prefer using Windows domain credentials.

 If you use local credentials, please make sure that the same Windows user accounts (with the same username and password) exist on both the system running the PRTG probe and the target computer. Otherwise the sensor cannot connect correctly.

Requirement: WSUS 3.0 Administration Console

 In order for this sensor to work, the Microsoft **WSUS 3.0 Administration Console** must be installed on the computer running the PRTG probe: either on the local system (on every node, if on a cluster probe), or on the system running the remote probe.

Add Sensor

The **Add Sensor** dialog appears when you [manually](#)^[325] add a new sensor to a device. It only shows the setting fields that are required for creating the sensor. Therefore, you will not see all setting fields in this dialog. You can change (nearly) all settings in the sensor's **Settings** tab later.

Sensor Settings

On the details page of a sensor, click the **Settings** tab to change its settings.

i Usually, a sensor connects to the **IP Address** or **DNS Name** of the parent device where you created this sensor. See the [Device Settings](#)^[402] for details. For some sensor types, you can define the monitoring target explicitly in the sensor settings. Please see below for details on available settings.

BASIC SENSOR SETTINGS

Sensor Name	Enter a meaningful name to identify the sensor. By default, PRTG shows this name in the device tree ^[181] , as well as in alarms ^[219] , logs ^[228] , notifications ^[3216] , reports ^[3252] , maps ^[3278] , libraries ^[3235] , and tickets ^[230] .
Parent Tags	Shows Tags ^[139] that this sensor inherits ^[140] from its parent device, group, and probe ^[133] . This setting is shown for your information only and cannot be changed here.
Tags	<p>Enter one or more Tags^[139], separated by spaces or commas. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. We recommend that you use the default value.</p> <p>You can add additional tags to the sensor if you like. Other tags are automatically inherited^[140] from objects further up in the device tree. These are visible above as Parent Tags.</p> <p>i It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>
Priority	Select a priority for the sensor. This setting determines where the sensor is placed in sensor lists. Top priority is at the top of a list. Choose from one star (low priority) to five stars (top priority).

SENSOR SETTINGS

WSUS Server Port	Enter the number of the port the WSUS server service runs on. The default value is 8530 . Please enter an integer value.
Connection Security	<p>Define if you want to use SSL encryption for the connection to the WSUS server or if you prefer unencrypted connections. Choose between:</p> <ul style="list-style-type: none"> ▪ Use SSL

SENSOR SETTINGS

- **Do not use any encryption**

 If you want to use SSL encryption, you have to configure your Windows Server Update Services (WSUS) accordingly. For details, see the Knowledge Base: [Can I encrypt connections to my WSUS server?](#)

DEBUG OPTIONS

Sensor Result

Define what PRTG will do with the sensor results. Choose between:

- **Discard sensor result:** Do not store the sensor result.
- **Write sensor result to disk (Filename: "Result of Sensor [ID].txt"):** Store the last result received from the sensor to the **Logs (Sensor)** directory in the PRTG data folder on the probe system the sensor is running on (on the Master node if in a cluster). File names: **Result of Sensor [ID].txt** and **Result of Sensor [ID].Data.txt**. This is for debugging purposes. PRTG overrides these files with each scanning interval.

 For more information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

 This option is not available when the sensor runs on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SENSOR DISPLAY

Primary Channel

Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel will always be displayed below the sensor's name. The available options depend on what channels are available for this sensor.

 You can set another primary channel later by clicking the pin symbol of a channel in the sensor's **Overview** tab.

Graph Type

Define how different channels will be shown for this sensor.

- **Show channels independently (default):** Show an own graph for each channel.

SENSOR DISPLAY

- **Stack channels on top of each other:** Stack channels on top of each other to create a multi-channel graph. This will generate an easy-to-read graph that visualizes the different components of your total traffic.
 - ⓘ This option cannot be used in combination with manual **Vertical Axis Scaling** (available in the [Sensor Channels Settings](#)³¹⁶⁰ settings).

Stack Unit

This setting is only available if stacked graphs are selected above. Choose a unit from the list. All channels with this unit will be stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all following settings are inherited from objects higher in the hierarchy and should be changed there, if necessary. Often, best practice is to change them centrally in the [Root](#)³³⁷ group's settings, see section [Inheritance of Settings](#)¹³⁷ for more information. To change a setting only for this object, disable inheritance by clicking the button next to **inherit from** under the corresponding setting name. You will then see the options described below.

SCANNING INTERVAL

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

Scanning Interval

Select a scanning interval (seconds, minutes, or hours) from the list. The scanning interval determines the time the sensor waits between two scans. You can change the available intervals in the [system administration](#)³³⁸⁵ on PRTG on premises installations.

If a Sensor Query Fails

Define the number of scanning intervals that a sensor has time to reach and check a device again in case a sensor query fails. The sensor can try to re-reach and check a device several times, depending on the option you select here, before it will be set to a **Down status**¹⁹⁵. This helps you avoid false alarms if the monitored device has only temporary issues. For previous scanning intervals with failed requests, the sensor will show a **Warning** status. Choose between:

- **Set sensor to "down" immediately:** The sensor will show an error immediately after the first failed request.

SCANNING INTERVAL

- **Set sensor to "warning" for 1 interval, then set to "down" (recommended):** After the first failed request, the sensor will show a yellow warning status. If the following request also fails, the sensor will show an error.
- **Set sensor to "warning" for 2 intervals, then set to "down":** Show an error status only after three consecutively failed requests.
- **Set sensor to "warning" for 3 intervals, then set to "down":** Show an error status only after four consecutively failed requests.
- **Set sensor to "warning" for 4 intervals, then set to "down":** Show an error status only after five consecutively failed requests.
- **Set sensor to "warning" for 5 intervals, then set to "down":** Show an error status only after six consecutively failed requests.

i Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval until they show an error. It is not possible to set a WMI sensor to "down" immediately, so the first option will not apply to these sensor types. All other options can apply.

i If a sensor has defined error limits for channels, it will always show a **Down** status immediately, so no "wait" option will apply.

i If a channel uses [lookup](#)³⁶⁹³ values, it will always show a **Down** status immediately, so no "wait" options will apply.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Inheritance for schedules, dependencies, and maintenance windows cannot be interrupted. The corresponding settings from the parent objects will always be active. However, you can define additional settings here. They will be active at the same time as the parent objects' settings.

Schedule

Select a schedule from the list. Schedules can be used to monitor for a certain time span (days, hours) every week. With the period list option it is also possible to pause monitoring for a specific time span. You can [create](#) new schedules and edit existing ones in the [account settings](#)³³¹¹.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

i Schedules are generally inherited. New schedules will be added to existing ones, so all schedules are active at the same time.

Maintenance Window

Specify if you want to set up a one-time maintenance window. During a "maintenance window" period, this object and all child objects will not be monitored. They will be in a paused state instead. Choose between:

- **Not set (monitor continuously):** No maintenance window will be set and monitoring will always be active.
- **Set up a one-time maintenance window:** Pause monitoring within a maintenance window. You can define a time span for a monitoring pause below and change it even for a currently running maintenance window.

i To terminate a current maintenance window before the defined end date, change the time entry in **Maintenance Ends** field to a date in the past.

Maintenance Begins

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the start date and time of the maintenance window.

Maintenance Ends

This field is only visible if you enabled the maintenance window above. Use the date time picker to enter the end date and time of the maintenance window.

Dependency Type

Define a dependency type. Dependencies can be used to pause monitoring for an object depending on the status of another. You can choose between:

- **Use parent:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency.
- **Select object:** Pause the current sensor if the device, where it is created on, is in **Down** status, or is paused by another dependency. Additionally, pause the current sensor if a specific other object in the device tree is in **Down** status, or is paused by another dependency. Select below.

SCHEDULES, DEPENDENCIES, AND MAINTENANCE WINDOW

- **Master object for parent:** Make this sensor the master object for its parent device. The sensor will influence the behavior of the device, where it is created on: If the sensor is in **Down** status, the device will be paused. For example, it is a good idea to make a Ping sensor the master object for its parent device to pause monitoring for all other sensors on the device in case the device cannot even be pinged. Additionally, the sensor will be paused if the parent group of its parent device is in **Down** status, or if it is paused by another dependency.

 Testing your dependencies is easy! Simply choose **Simulate Error Status** from the context menu of an object that other objects depend on. A few seconds later all dependent objects should be paused. You can [check all dependencies](#)^[3209] in your PRTG installation by selecting **Devices | Dependencies** from the main menu bar.

Dependency This field is only visible if the **Select object** option is enabled above. Click on the reading-glasses and use the [object selector](#)^[240] to choose an object on which the current sensor will depend.

Dependency Delay (Sec.) Define a time span in seconds for a dependency delay. After the master object for this dependency goes back to **Up** status, PRTG will start monitoring the depending objects after this extra delayed. This can help to avoid false alarms, for example, after a server restart, by giving systems more time for all services to start up. Please enter an integer value.

 This setting is not available if you choose this sensor to **Use parent** or to be the **Master object for parent**. In this case, please define delays in the parent [Device Settings](#)^[402] or in the superior [Group Settings](#)^[375].

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)¹³⁷ for more information.

User Group Access

Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)¹⁵⁸.

CHANNEL UNIT CONFIGURATION

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

Channel Unit Types For each type of sensor channel, define the unit in which data is displayed. If defined on probe, group, or device level, these settings can be inherited to all sensors underneath. You can set units for the following channel types (if available):

- **Bandwidth**
- **Memory**
- **Disk**
- **File**
- **Custom**

 Custom channel types can be set on sensor level only.

More

Knowledge Base: Which .NET version does PRTG require?

- <https://kb.paessler.com/en/topic/60543>

Knowledge Base: Can I encrypt connections to my WSUS server?

- <https://kb.paessler.com/en/topic/63611>

Edit Sensor Channels

To change display settings, spike filter, and limits, switch to the sensor's **Overview** tab and click the gear icon of a specific channel. For detailed information, see the [Sensor Channels Settings](#)^[316] section.

Notifications

Click the **Notification Triggers** tab to change notification triggers. For detailed information, see the [Sensor Notification Triggers Settings](#)^[317] section.

Others

For more general information about settings, see the [Object Settings](#)^[217] section.

7.9 Additional Sensor Types (Custom Sensors)

You can create and use your own, self-written custom sensors in PRTG Network Monitor to go far beyond the PRTG standard sensor set. You can create your own sensors using Windows Management Instrumentation Query Language (WQL), visual basic scripting, PowerShell, batch scripting, SQL queries, by compiling an EXE or DLL file (using any Windows software development tool), by running Python scripts, or by translating JSON and XML responses of a REST API into sensor values.

 You cannot use custom sensors on hosted probes in PRTG hosted by Paessler (except SSH sensors). If you want to use custom sensors, please add them to a remote probe device.

Basics

For a general introduction, see the sections about EXE/Script sensors and the [API documentation](#)^[3637], which contains details about the necessary return format for these sensors. WMI Custom sensors allow executing WQL requests.

- [EXE/Script Sensor](#)^[834]
- [EXE/Script Advanced Sensor](#)^[847]
- [Python Script Advanced Sensor](#)^[1597]
- [REST Custom Sensor](#)^[1646]
- [SSH Script Sensor](#)^[2607]
- [SSH Script Advanced Sensor](#)^[2622]
- [Application Programming Interface \(API\) Definition](#)^[3606]
- [WMI Custom Sensor](#)^[2967]
- [WMI Custom String Sensor](#)^[2877]

Additionally, some types of SQL sensors execute script files with SQL queries:

- [Microsoft SQL v2 Sensor](#)^[1267]
- [MySQL v2 Sensor](#)^[1284]
- [Oracle SQL v2 Sensor](#)^[1457]
- [PostgreSQL Sensor](#)^[1574]

The [HL7 Sensor](#)^[944] sends messages that are stored in extra files on the probe system.

Custom Sensors Included in PRTG

After installing PRTG Network Monitor, you will already find a selection of custom EXE/Script, Python, and WMI WQL script sensors in the [PRTG program directory](#)^[3734], as well as scripts with SQL queries for specific [database sensors](#)^[3155], REST configuration files in JSON template (*.template) format for the [REST Custom sensor](#)^[1646], and HL7 message files for the [HL7 sensor](#)^[944]. Many of the files are sample projects that you can edit and improve for your needs.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXE

- Demo Batchfile - Returns 200.bat
- Demo Batchfile - Set sensorstate to error.bat
- Demo Batchfile - Set sensorstate to warning.bat
- Demo Cmd - Returns 200.cmd
- Demo Dll - Returns a random integer.dll
- Demo EXE - Returns a random integer.exe
- Demo EXE - Returns number of files in folder (parameter).exe
- Demo EXE - Returns user of process.exe
- Demo Powershell Script - Available MB via WMI.ps 1
- Demo Powershell Script - InterruptsPerSec via WMI.ps 1
- Demo Powershell Script - Powershell Version.ps 1
- Demo Powershell Script - Returns a fixed integer value.ps 1
- Demo Powershell Script - Returns a random integer value.ps 1
- Demo Powershell Script - Returns Random Integer and Warnings.ps 1
- Demo VBScript - InterruptsPerSec via WMI.vbs
- Demo VBScript - Multiplies two integers(2 parameters).vbs
- Demo VBScript - Returns a fixed float value.vbs
- Demo VBScript - Returns a fixed integer value.vbs
- Demo VBScript - Returns a random value.vbs
- Demo VBScript - Returns number of svchost processes.vbs
- Demo VBScript - Returns user of process.vbs
- Demo VBScript - Returns warning depending on number of svchost processes.vbs
- Demo VBScript - Timezone via WMI.vbs
- Demo VBScript - UTCTime via WMI.vbs
- Load_Test_CPU_1_Mio_Primes.exe
- Load_Test_CPU_10_Mio_Primes.exe
- Load_Test_Disk_Write_Read_1000_files.exe
- Load_Test_Disk_Write_Read_10000_files.exe
- Load_Test_Memory_Allocate_And_Free_400MB.exe

To create a new sensor based on one of these files, create a new [EXE/Script Sensor](#)⁸³⁴ and choose the respective file from the **EXE/Script** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\EXEXML

- Demo Batchfile - Returns static values in four channels.bat

To create a new sensor based on one of these files, create a new [EXE/Script Advanced Sensor](#)⁸⁴⁷ and choose the respective file from the **EXE/Script** list in the sensor settings.

HL7 Message Files Included in PRTG—Folder: \Custom Sensors\hl7

- ADT_A08.hl7
- ORM_O01.hl7

Each file contains an HL7 message that is conform to the HL7 message format. To create a new sensor based on one of these files, create a new [HL7 Sensor](#)⁹⁴⁴ and choose the respective file from the **HL7 Messages** list in the sensor settings. You can override certain message headers in the files via the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\python

- sensor_example.py

This Python example script just returns fixed values in two channels to demonstrate the usage. To create a new sensor based on this file, create a new [Python Script Advanced Sensor](#)¹⁵⁹⁷ and choose the file from the **Python Script** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\rest

- kemp.loadbalancer.template: maps values returned by the RESTful API of a KEMP load balancer to sensor channels, for example, CPU usage, memory usage, traffic
- prtgsensorstats.template: maps values returned by the API of your PRTG installation to sensor channels that show the count of each sensor status on the local probe
- windows.docker.container.stats.template: maps values returned by the Docker Engine API to sensor channels, for example, CPU usage, memory usage, traffic, I/O
- wunderground.template: maps values returned by the Weather Underground API to sensor channels, for example, temperature, dew point, pressure, wind speed, wind direction

To create a new sensor based on one of these files, create a new [REST Custom Sensor](#)¹⁶⁴⁶ on the device that provides the REST API and choose the file from the **REST Configuration File** list in the sensor settings.

SQL Query Files Included in PRTG—Folder: \Custom Sensors\sql\<dbms>

- Demo Serveruptime.sql

You can find this demo SQL query script in each subfolder for each supported **database management system (dbms)**: \mssql, \mysql, \oracle, \postgres

To create a new sensor that uses one of the scripts in the dbms folders, create the according sensor type ([see above for supported sensors](#)³¹⁵⁸) and choose the respective file from the **SQL Query File** list in the sensor settings.

Custom Sensors Included in PRTG—Folder: \Custom Sensors\WMI WQL scripts

- Demo WQL Script - Get Win32LogicalDiscFreeMB.wql
- Demo WQL Script - Get Win32OsBuildnumber.wql
- Demo WQL Script - Get Win32PercentProcessorIdleTime.wql
- Demo WQL Script - Get Win32PercentProcessorTime.wql

To create a new sensor based on one of these files, create a new [WMI Custom Sensor](#)²⁹⁶⁷ and choose the respective file from the **WQL File** list in the sensor settings.

Downloading Pre-Built Custom Sensors

Good resources to find custom sensors that PRTG users and we from Paessler share are the [PRTG Script World](#) and our Knowledge Base. In the Knowledge Base, search for the tag **custom-script-exe** to find a lot of custom sensors: <https://kb.paessler.com/en/tags/custom-script-exe/>

More

You can find useful scripts for sensors in the **PRTG Script World**:

- <https://www.paessler.com/script-world>

For the other sensor types that work out-of-the-box, see

- [List of Available Sensor Types](#)⁴²⁹

Knowledge Base: Guide for PowerShell Based Custom Sensors

- <https://kb.paessler.com/en/topic/71356>

Knowledge Base: Custom sensors

- <https://kb.paessler.com/en/tags/custom-script-exe/>

Knowledge Base: How can I share my self-written PRTG script/program with other PRTG users?

- <https://kb.paessler.com/en/topic/63737>

Knowledge Base: How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?

- <https://kb.paessler.com/en/topic/11283>

Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- <https://kb.paessler.com/en/topic/75372>

Sensor Settings Overview

For information about sensor settings, see the following sections:

- [Sensor Settings—List of Available Sensor Types](#)
- [Additional Sensor Types \(Custom Sensors\)](#)
- [Sensor Channels Settings](#)
- [Sensor Notification Triggers Settings](#)

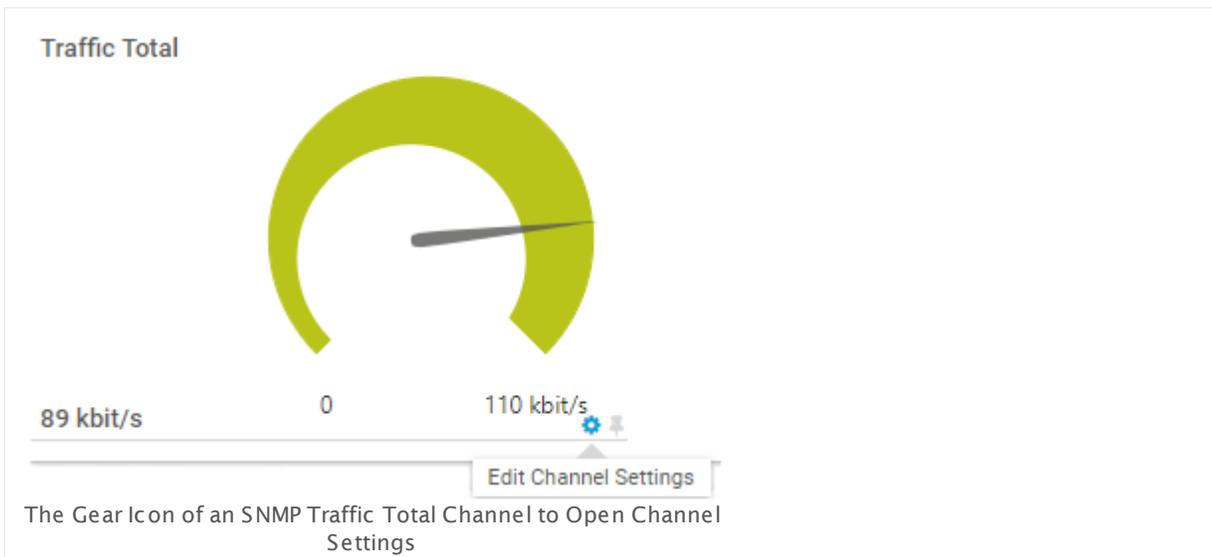
7.10 Sensor Channels Settings

A sensor has one or more channels in which it handles the actual monitoring data. In the channel settings, you can define how to display the data from the sensor's different channels displayed in graphs, gauges, and tables. Additionally, the channel data can determine the [sensor status](#)¹⁹⁵. Use the limit settings to define desired sensor states for values.

On the sensor's **Overview** tab, click the gear icon of a specific channel gauge to change its settings. Click the pin symbol on the right of the gear icon in a gauge to make this channel the primary channel of the selected sensor.

You can also open the settings of a channel by clicking the gear icon in the channels data table.

i For [lookup](#)³⁶⁹³ channels, we recommend that you stay below 120 lookup values to get expressive gauges. For non-primary lookup channels, the upper limit is around 40 lookup values.



The available options are nearly the same for all sensor types. An exception applies to the **Downtime** channel, which is automatically calculated and does not offer all settings. Channels with **absolute** values additionally have an option to define the **Value Mode**. Custom channels have a **Value Lookups and Limits** setting to distinguish between alerting by lookups or numerical limits.

You can quickly choose another channel of the selected sensor via the dropdown list at the top of the channel settings list.

Edit Channel ✕

Free Space (ID 0) ▼

Edit Channel "Free Space"

Name ⓘ
Free Space

ID ⓘ
0

Graph Rendering ⓘ
 Show in Graphs
 Hide from Graphs

Table Rendering ⓘ
 Show in Tables
 Hide from Tables

Line Color ⓘ
 Automatic
 Manual

Line Width ⓘ
1

Value Mode ⓘ
 Average
 Minimum
 Maximum

Decimal Places ⓘ
 Automatic
 All
 Custom

Spike Filter ⓘ
 Disable Filtering
 Enable Filtering

Vertical Axis Scaling ⓘ

Channel Settings for a Disk Sensor

Available Channel Settings

EDIT CHANNEL	
Name	<p>Enter a meaningful name to identify the channel (not editable for script sensors after sensor creation). The name will appear in graphs and tables.</p> <p>i You can automatically add the sensor's ID to the name by using the placeholder <code>[#id]</code>.</p>
Unit	<p>This field is only visible for custom sensors.</p> <p>Enter the unit for the values that this sensor returns. Please enter a string. This unit string is used for display purposes and will be shown in graphs, data tables, and gauges. If you want to change the Unit after having created the sensor, you can change it in the sensor's channel settings³¹⁶⁰.</p>
Scaling Multiplication	<p>This field is only visible for channels with a custom unit. If you want to multiply the received raw data by a certain value, enter the multiplier here. Otherwise, use the default value 1 to not change the received value. Please enter an integer value.</p> <p>i The following sensor types provide the scaling factor for received values with custom units in their sensor settings.</p> <ul style="list-style-type: none"> ▪ Sensor Factory Sensor¹⁷²² (you can use multiplication and division in the channel definition) ▪ SNMP APC Hardware Sensor¹⁸³¹ ▪ SNMP Custom Sensor¹⁹⁵⁰ ▪ SNMP Dell Hardware Sensor²⁰³⁴ ▪ WMI Custom Sensor²⁸⁶⁹
Scaling Division	<p>This field is only visible for channels with a custom unit. If you want to divide the received raw data by a certain value, enter the divisor here. Otherwise, use the default value 1 to not change the received value. Please enter an integer value.</p> <p>i The following sensor types provide the scaling factor for received values with custom units in their sensor settings.</p> <ul style="list-style-type: none"> ▪ Sensor Factory Sensor¹⁷²² (you can use multiplication and division in the channel definition) ▪ SNMP APC Hardware Sensor¹⁸³¹ ▪ SNMP Custom Sensor¹⁹⁵⁰ ▪ SNMP Dell Hardware Sensor²⁰³⁴

EDIT CHANNEL

	<ul style="list-style-type: none"> ▪ WMI Custom Sensor ²⁶⁶⁹
ID	<p>Shows the ID of the channel. You cannot change the ID. PRTG uses it for unique identification. For example, you need the ID when using Sensor Factory ¹⁷²⁰ sensors.</p> <p>There are a few special, fixed channel IDs.</p> <ul style="list-style-type: none"> ▪ -1 is for sum channels of traffic sensors (for example, of the SNMP Traffic Sensor ²⁴⁶⁷). ▪ -4 is for the Downtime channel (you can use it, for example, for an uptime percentage calculation in a Sensor Factory Sensor ¹⁷²⁰). ▪ -2 (coverage) and -3 (error) are internally used.
Limits	<p>This setting is not available for custom channels.</p> <p>Define if you want to use thresholds for this channel. The channel can affect the status of the sensor ¹⁹⁵¹ it is part of. With limits you can define when the sensor will show a Warning or Down status, depending on the channel data. For example, you can use this function to set a traffic sensor (which is usually never in a down state) to error when the monitored values reach critical limits.</p> <p>Choose between:</p> <ul style="list-style-type: none"> ▪ Disable Limits: Do not use the channel data to control the sensor status. ▪ Enable alerting based on limits: Define limits for numerical values returned by the device. Additional fields appear below. The sensor of this channel will enter a Warning or Down status when limits are undercut or overrun. <p>i The limits option is not available for the Downtime channel.</p> <p>i You can show limits in graphs (highlighted in yellow or red) if you select exactly one channel with a limit in a graph.</p>
Value Lookups and Limits	<p>This setting is only available for custom channels.</p> <p>Define when the channel will show a down status and alert you, either based on the lookup definition or based on thresholds for returned values. Only the option that you choose will apply. For example, if you choose limits as alerting method, an error status defined the lookups will not show up.</p> <p>Choose between:</p>

EDIT CHANNEL

- **Enable alerting based on lookups:** Use the lookup definition of the channel to control the sensor status. Make sure the channel uses a proper **Value Lookup** if you choose this option. Select the lookup file either in the channel settings below or in the sensor settings, depending on the sensor type. If you do not want to use the channel data to control the sensor status, select **None** as **Value Lookup**.
- **Enable alerting based on limits:** Define limits for numerical values returned by the device. Additional fields appear below. The sensor of this channel will enter a **Warning** or **Down** status when limits are undercut or overrun.

 If you choose limit-based alerting, errors and warnings that you have defined in the lookup file will not apply!

Value Lookup

This field is only visible for custom sensors and if you select lookups-based alerting. Select the [lookup](#) file that you want to use with this channel.

 Do not use this option for sensors that provide the unit **Value Lookup** in the sensor settings! The channel setting will be overwritten with the next sensor scan. Please define the lookup file that you want to use with this channel on the **Settings** tab of the sensor. Choose the option **Value Lookup** for the setting **Sensor Channel #x Unit** (where **x** is the number of the channel) and choose the desired lookup file under **Sensor Channel #x Value Lookup**. See manual section [Define Lookups—Requirement: Channel Unit "Custom"](#) for affected sensor types.

 If you choose **None**, alerting by lookups and limits will be disabled and channels will not appear as lookup. If you want to keep the lookup representation without alerting, define the states accordingly in the lookup file.

Upper Error Limit [unit]

This field is only visible if you enable limits above. Specify an upper limit for a **Down status**. If the channel values overrun this value, the sensor will be **Down**. Please enter a valid number into at least one of the limit fields.

 While a sensor shows a **Down** status triggered by a limit, it will still receive data in its channels.

Upper Warning Limit [unit]

This field is only visible if you enable limits above. Specify an upper limit for a **Warning status**. If the channel values overrun this value, the sensor will be **Warning**. Please enter a valid number into at least one of the limit fields.

EDIT CHANNEL

Lower Warning Limit [unit]	This field is only visible if you enable limits above. Specify a lower limit for a Warning status ¹⁹⁵ . If the channel values undercut this value, the sensor will be Warning . Please enter a valid number into at least one of the limit fields.
Lower Error Limit [unit]	<p>This field is only visible if you enable limits above. Specify a lower limit for a Down status ¹⁹⁵. If the channel values undercut this value, the sensor will be Down. Please enter a valid number into at least one of the limit fields.</p> <p>i While a sensor shows a Down status ¹⁹⁵ triggered by a limit, it will still receive data in its channels.</p>
Error Limit Message	This field is only visible if you enable limits above. Enter an additional message. It will be added to the sensor message when showing a Down status ¹⁹⁵ . Please enter a string or leave the field empty.
Warning Limit Message	This field is only visible if you enable limits above. Enter an additional message. It will be added to the sensor message when showing a Warning status ¹⁹⁵ . Please enter a string or leave the field empty.
Graph Rendering	<p>Define if you want to show this channel in data graphs ²⁰¹. Choose between:</p> <ul style="list-style-type: none"> ▪ Show in Graphs: Sensor graphs contain the data of this channel. ▪ Hide from Graphs: Sensor graphs do not contain data of this channel. <p>i If you choose to hide this channel in graphs, it also will not appear in the graph of a Report ³²⁵².</p>
Table Rendering	<p>Define if you want to show this channel in data tables ¹⁹⁸. Choose between:</p> <ul style="list-style-type: none"> ▪ Show in Tables: Sensor data tables contain the data of this channel. ▪ Hide from Tables: Sensor data tables do not contain the data of this channel. This option hides the channel gauge as well, but the channel will still be available in the data table of the sensor's Overview tab. <p>i If you choose to hide this channel in data tables, PRTG also will not use it for the calculation of the "sum" (total) channel of a sensor. It also will not appear in data tables of a Report ³²⁵².</p>

EDIT CHANNEL

Line Color	<p>Define the color of the channel display in graphs. Choose between:</p> <ul style="list-style-type: none">▪ Automatic: PRTG sets the color of this channel in graphs automatically.▪ Manual: Individually define the color of this channel. You can enter the desired color code below.
Color (#rrggbb)	<p>This option is only available if you choose manual line color above. Enter a color in hexadecimal RGB notation as in HTML and CSS, or choose a color from the visual color selector. The field with the hexadecimal color value will change to the selected color automatically.</p>
Line Width	<p>Define the width of the channel line in graphs. Enter an integer value in pixels. The maximum line width is 25 px, but we recommend that you use values between 1 and 7 only to get optimal results.</p>
Data	<p>This setting is available for most channels. Define how to display data. Choose between:</p> <ul style="list-style-type: none">▪ Display actual values in [unit]: Display the values in the shown unit.▪ Display in percent of maximum: Calculate and show percent values based on a maximum value. Provide a maximum below.  If you choose this option, you cannot display the data of traffic sensors as a positive and negative area graph.
Maximum ([unit])	<p>This field is only visible if you choose the percent of maximum setting above. Enter a value to use as maximum. Please consider the given unit. PRTG will calculate all percent values based on this value.</p> <p>Please enter an integer value.</p>
Value Mode	<p>This setting is only available for sensor channels that return absolute values. It is not available for sensors showing difference values, such as traffic channels. Depending on this setting, the channel cannot only show averages, but also minimum or maximum values in the graphs for the respective time spans.</p> <p>Choose between:</p> <ul style="list-style-type: none">▪ Average: The channel shows average values.▪ Minimum: The channel shows minimum values.▪ Maximum: The channel shows maximum values.

EDIT CHANNEL

 See the Knowledge Base for more information about value modes: [What is the Value Mode in channel settings?](#)

Decimal Places

Define how many decimal places of the channel's data to display in graphs and tables. Choose between:

- **Automatic:** PRTG automatically defines how many decimal places are used for optimal viewing results.
 -  Values between 10 and -10 are rounded to two decimal places. Values that are very close to an integer are rounded to the integer, for example, 3.001 is rounded to 3.
- **All:** Display all available decimal places.
- **Custom:** Manually define the number of decimal places. If you choose this option, an additional field will appear. Please enter an integer value.

Spike Filter

You can use a spike filter to correct faulty monitoring data. Sometimes, sensors report enormously high or far too low values. This can be because of an error in data transmission, or because of incompatibilities of the physical device you are monitoring. This can make graphs unreadable. A spike filter can compensate for these flaws.

If you enable a spike filter, values above and below a certain limit are disregarded in the monitoring data for graphs and tables.

Choose between:

- **Disable Filtering:** Display all data as it is received. Do not filter out spikes.
- **Enable Filtering:** Enable a filter to remove spike values. Additional fields appear below.
 -  This does not change monitoring data itself but only the presentation of the data. This setting is valid for all data of this channel, including historic data.
 -  The spike filter option is not available for the channel **Downtime**.

Spike Filter Max. Value
[unit]

This field is only visible if you enable the spike filter above. Enter the maximum value to show in the channel data. PRTG will disregard all data above this value in graphs and tables. Please enter an integer value or leave the field empty.

Spike Filter Min. Value
[unit]

This field is only visible if you enable the spike filter above. Enter the minimum value to show in the channel data. PRTG will disregard all data below this value in graphs and tables. Please enter an integer value or leave the field empty.

EDIT CHANNEL

Vertical Axis Scaling	<p>Define how to display the vertical axis for the channel in graphs. Choose between:</p> <ul style="list-style-type: none"> ▪ Automatic Scaling: PRTG automatically uses the optimum scaling. Usually the scaling ranges from the minimum to the maximum value. PRTG uses one single scale for each unit label only. ▪ Manual Scaling: Define the scaling manually. Additional fields appear below. Defining manual axis scaling can make low values better visible in your graph, but it may result in a graph with multiple vertical axes for the same unit label. <p> Settings for this option are ignored if you enable the Chart Type Stack channels on top of each other or Show in and out traffic as positive and negative area chart (available for traffic sensors) on the sensor's Settings tab.</p>
Vertical Axis Maximum [unit]	This field is only visible if you enable vertical axis scaling above. Enter the maximum value to use on the vertical axis for the channel. Please enter an integer value.
Vertical Axis Minimum [unit]	This field is only visible if you enable vertical axis scaling above. Enter the minimum value to use on the vertical axis for the channel. Please enter an integer value.

 Click **Ok** to save your settings and to close the settings window. Click **Apply** to save the changed settings while the **Edit Channel** window remains open. This functionality is useful if you want to change the settings of other channels of the current sensor as well. You can select another channel via the dropdown menu above the settings. You can close the settings window without saving by clicking **Cancel**.

 If you have changed any settings and click **Cancel** or choose another channel via the dropdown menu without applying the changes, PRTG will ask you to confirm this step. **Discard Changes** will ignore any edits and closes the window or shows the settings of another selected channel. Click **Save** to apply your changes.

More

Knowledge Base: What is the Value Mode in channel settings?

- <https://kb.paessler.com/en/topic/60238>

Sensor Settings Overview

For information about sensor settings, see the following sections:

- [Sensor Settings—⁴²⁸List of Available Sensor Types⁴²⁹](#)

- [Additional Sensor Types \(Custom Sensors\)](#)  3155
- [Sensor Channels Settings](#)  3160
- [Sensor Notification Triggers Settings](#)  3170

7.11 Sensor Notification Triggers Settings

The status or the data of a sensor can trigger notifications. Using this mechanism, you can configure external alerting tailored to your needs.

Example of Notification Trigger Settings

Although the sensors activate a notification trigger, you can set notification triggers higher in the hierarchy (for example, for groups or devices). Because of this you can define notification triggers for multiple sensors using the [inheritance mechanism](#)^[137]. Monitoring objects with inherited notification triggers show these in section **Triggers That Can Be Inherited From Parent Object(s)** on the **Notification Triggers** tab.

PRTG already includes a default notification trigger for the [Root Group](#)^[133]. This default notification trigger provokes the standard notification **Email and push notification to admin** if there is any [sensor in down status](#)^[195] in your PRTG installation for at least 10 minutes.

You can also define notification triggers in [Libraries](#)^[326]. Sensors that are in a library with defined notification triggers show these notification triggers in section **Triggers That Are Defined in Library Object(s)** on the **Notification Triggers** tab.

Note

This section describes one of four steps to set up the notification system in PRTG. To complete your notification setup, go through all of the following steps:

1. Check and set up the **Notification Delivery** settings to define how and to which recipient PRTG will send messages.
For detailed information, see [System Administration—Notification Delivery](#)³³⁶¹.
2. Check and set up **Notification Contacts** for the PRTG users to define the recipients of notifications.
For detailed information, see [Account Settings—Notification Contacts](#)³³³⁴.
3. Check and set up **Notification Templates** to define the notification methods and their content.
For detailed information, see [Account Settings—Notification Templates](#)³³¹¹.
4. Check and set up **Notification Triggers** for objects to define when notification messages will be sent.
For detailed information, see [Sensor Notification Triggers Settings](#)³¹⁷⁰.

 We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one [email notification](#)³³¹⁷ and one [SMS notification](#)³³²⁰. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a [state trigger](#)³¹⁷² and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

 For background information, see the [Notifications](#)³²¹⁶ section.

Available Notification Triggers Settings

On an object's detail page, open the **Notification Triggers** tab to change sensor notification triggers. The available options are the same for all objects. When defining triggers for probes, groups, or devices, they can be inherited down to sensor level.

TRIGGERS THAT CAN BE INHERITED FROM PARENT OBJECT(S)

You see a list of all notification triggers that are defined higher in the hierarchy. The list is empty and shows the message (**no triggers defined**) when you have not set any triggers in probes, groups, or devices above the current object in the [Object Hierarchy](#)¹³³¹. You can see the **Type** of trigger and the notification **Rule** that the monitoring object executes once this trigger is activated.

Trigger Inheritance	<p>Define if you want to use the triggers shown above on the current object. Choose between:</p> <ul style="list-style-type: none"> ▪ Inherit all triggers from parent objects and use the triggers defined above: Use the triggers shown above. If the defined condition is met, the corresponding trigger is activated and the notification provoked. Click the notification name to open its settings page³³¹¹. Click the name of the monitoring object in the column Inherited from to open its Overview tab. ▪ Only use triggers defined above: Do not use the triggers shown above. Only use the triggers that you define above in section Notification Triggers for this object.
---------------------	---

TRIGGERS THAT CAN BE INHERITED FROM PARENT OBJECT(S)

This setting is valid for all triggers shown above. It is not possible to only select some of the triggers.

In section **Triggers that are defined in library object(s)** you see all notification triggers that are set for [Libraries](#)³²³⁶ that contain the currently selected sensor.

TRIGGERS THAT ARE DEFINED IN LIBRARY OBJECT(S)

You see a list of all notification triggers that are defined in libraries that include the currently selected sensor. The list is empty and shows the message (**no triggers defined**) when you have not set any triggers in libraries that contain the current sensor. You can see the **Type** of trigger and the notification **Rule** that the sensor executes once this trigger is activated.

Click the notification name to open its [settings page](#)³³¹¹. Click a library name in the column **Inherited from** to view this library.

 You cannot turn off trigger usage for the current sensor from a library here. If you do not want to use any notification triggers from a library for this sensor, open the library and remove this sensor from it or refine the triggers on the [Notification Triggers](#)³²⁵⁰ tab.

You can set up one or more of the following triggers, each with different setting options. Which trigger types are visible depends on the kind of object you edit:

- [Add State Trigger](#)³¹⁷²
- [Add Speed Trigger](#)³¹⁷⁴
- [Add Volume Trigger](#)³¹⁷⁷
- [Add Threshold Trigger](#)³¹⁷⁸
- [Add Change Trigger](#)³¹⁸⁰

You can create all notification triggers by forming sentences in "natural language". There are different options available for every type.

Add State Trigger

Define a trigger that is activated when a sensor changes its current status. This is the most common reason to send out notifications. Hover over  and select **Add State Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more [notification\(s\)](#)³³¹¹ to be executed.

STATE TRIGGER

When sensor state is [...]

Select the condition that will trigger the notification. The trigger will be activated when a sensor enters the selected [status](#)^[195]. Choose from the dropdown menu:

- **Down:** The trigger is activated if a sensor changes to a **Down** status.
- **Warning:** The trigger is activated if a sensor changes to a **Warning** status.
- **Unusual:** The trigger is activated if a sensor changes to an **Unusual** status.
- **Partial Down:** The trigger is activated if a sensor changes to a **Down (Partial)** status (available in a [cluster](#)^[130] configuration).
- **Up:** The trigger is activated if a sensor changes to an **Up** status.
- **Unknown:** The trigger is activated if a sensor changes to an **Unknown** status.

...for at least [...] seconds

Define how many seconds PRTG waits before it sends out a notification (**latency**). This can avoid false alarms if a sensor 'flickers' and, for example, changes to a down status for just a few seconds. If the selected condition (the sensor status) persists after the defined time in seconds, the notification is triggered. Please enter an integer value.

 Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case.

...perform [...]

Select a notification that PRTG sends out if the selected condition (the sensor status) is true **and** the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the [Account Settings—Notification Templates](#)^[331] settings. You can also choose **no notification** to only use other conditions for this trigger.

When sensor state is [...] for at least [...] seconds

Define an escalation latency in seconds. This "escalation" triggers a second notification if the number of seconds you enter here has passed since the sensor status has entered the defined condition. Use this to automatically escalate a notification in case a problem persists for a longer time. Please enter an integer value.

 PRTG automatically takes the status from the first trigger condition above.

STATE TRIGGER

...perform [...]	<p>Select a (second) notification that PRTG sends out if the selected condition (the sensor status) is true and the escalation latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notification Templates settings. You can also choose no notification to only use other conditions for this trigger.</p> <p>i Select a notification with another delivery method than above to ensure the delivery in case of technical issues with the first notification.</p>
...and repeat every [...] minutes	<p>Define an interval in minutes in which PRTG sends the escalation notification (defined above) repeatedly. The second (escalation) notification defined will be resent every x minutes that you enter here. Please enter an integer value.</p> <p>i If you enter 0, PRTG will not send repeating escalation notifications.</p>
When condition clears after a notification was triggered perform [...]	<p>Select a notification that PRTG sends out if the selected condition (the sensor status) is not true anymore because the sensor status changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notification Templates settings. You can also choose no notification to only use other conditions for this trigger.</p> <p>i PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select no notification above, you will get the notification about the cleared condition nevertheless if you define it here. The definition of an "escalation" notification does not influence notifications for cleared conditions.</p>
Save	Click Save to confirm your settings.
Cancel	Click Cancel to undo your changes.

Add Speed Trigger

Define a trigger that is activated when the currently monitored speed in a sensor changes (for example, a traffic sensor). Hover over **+** and select **Add Speed Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more [notification\(s\)](#) to be executed.

SPEED TRIGGER

When [...] channel	From the dropdown menu, select the channel whose data PRTG considers for speed comparison. Select Primary to generally use the primary channel of a sensor (you can define this in the sensor settings ⁴²⁸), or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger are based on the chosen channel.
...is [...]	Select the condition that will trigger the notification. Choose from the dropdown menu: <ul style="list-style-type: none">▪ Above: The trigger is activated if the value of the selected channel exceeds a defined value.▪ Below: The trigger is activated if the value of the selected channel falls below a defined value.▪ Equal to: The trigger is activated if the value of the selected channel is the same as a defined value.▪ Not Equal to: The trigger is activated if the value of the selected channel is different than a defined value.
[value]	Define the value to which PRTG compares the channel data. Please enter an integer value.
[scale]	From the dropdown menu, select the unit in which you entered the [value] above. [scale] and [time] together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally. Choose from: <ul style="list-style-type: none">▪ bit▪ kbit▪ Mbit▪ Gbit▪ Tbit▪ Byte▪ KByte▪ MByte▪ GByte▪ TByte
[time]	Select the time for the scale (so you create a scale per time unit). Choose from the dropdown menu:

SPEED TRIGGER

- **second**
- **minute**
- **hour**
- **day**

[scale] and **[time]** together define the unit for the given value. If the channel data is shown in a different unit PRTG will automatically convert values internally.

..for at least [...] seconds

Define how many seconds PRTG waits before it sends out a notification (**latency**). This can avoid false alarms if a channel reaches a limit for just a few moments. If the combined channel condition of **[value]**, **[scale]**, and **[time]** persists after the defined time span, the notification will be triggered. Please enter an integer value.

 Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case.

...perform [...]

Select a notification that is triggered if the combined channel condition of **[value]**, **[scale]**, and **[time]** is true **and** the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the [Account Settings—Notification Templates](#)³³¹¹ settings. You can also choose **no notification** to only use other conditions for this trigger.

When condition clears perform [...]

Select a notification that is triggered if the combined channel condition of **[value]**, **[scale]**, and **[time]** is **not** true anymore because the channel value has changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the [Account Settings—Notification Templates](#)³³¹¹ settings. You can also choose **no notification** to only use other conditions for this trigger.

 PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select **no notification** above, you will get the notification about the cleared condition nevertheless if you define it here.

Save

Click **Save** to confirm your settings.

Cancel

Click **Cancel** to undo your changes.

 No escalation notification and no repeat are available for this trigger type.

Add Volume Trigger

Define a trigger that is activated when a sensor (for example, a traffic sensor) reaches a certain volume limit in a specified time. Hover over  and select **Add Volume Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more [notification\(s\)](#)³³¹¹ to be executed.

VOLUME TRIGGER

When [...] channel From the dropdown menu, select the channel whose data PRTG considers for this comparison. Select **Primary** to generally use the primary channel of a sensor (you can define this in the [sensor settings](#)⁴²⁸), or choose a specific channel name from the list (there are different channels for every sensor type). All following settings for this trigger are based on the chosen channel.

...has reached [value] Define the value to which PRTG compares the channel data. If the channel data exceeds this value, a notification is triggered. Please enter an integer value.

[scale] From the dropdown menu, select the unit in which you entered the **[value]** above. **[scale]** and **[time]** together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally. Choose between:

- **Byte**
- **KByte**
- **MByte**
- **GByte**
- **TByte**

per [time] Select the time for the scale (so you create a scale per time designation). Choose from the dropdown menu:

- **Hour**
- **Day**
- **Week**
- **Month**

[scale] and **[time]** together define the unit for the given value. If the channel data is shown in a different unit, PRTG will automatically convert values internally.

VOLUME TRIGGER

...perform [...]	Select a notification that is triggered if the [value] in the combined unit of [scale] and [time] is exceeded. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notification Templates settings. You can also choose no notification to only use other conditions for this trigger.
Save	Click Save to confirm your settings.
Cancel	Click Cancel to undo your changes.

 No escalation notification, no repeat, and no notification when condition clears are available for this trigger type.

Add Threshold Trigger

Define a trigger that is activated when a sensor reaches specific values. Hover over  and select **Add Threshold Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing notification to change it. Define the settings as described below. Every trigger provokes one or more [notification\(s\)](#) to be executed.

THRESHOLD TRIGGER

When [...] **channel** From the dropdown menu, select the channel whose data PRTG will consider for the comparison. Select **Primary** to generally use the primary channel of a sensor. You can define the primary channel in the [sensor settings](#). Choose a specific channel name from the list to apply the trigger to this sensor channel. There are different channels for every sensor type.

All following settings for this trigger are based on the chosen channel.

 The threshold trigger for a **Total** channel defined on device or group level or defined in [libraries](#) only applies to the sum channel of traffic sensors. This channel has ID -1. The trigger works with the **Total** channel of the following sensors:

- Amazon CloudWatch EBS
- IPFIX
- IPFIX (Custom)
- jFlow V5
- jFlow V5 (Custom)

THRESHOLD TRIGGER

- NetFlow V5
- NetFlow V5 (Custom)
- NetFlow V9
- NetFlow V9 (Custom)
- Packet Sniffer
- sFlow
- sFlow (Custom)
- SMTP&IMAP Round Trip
- SMTP&POP3 Round Trip
- SNMP Traffic
- Windows Network Card

...is [...]

Select the condition that will trigger the notification. Choose from the dropdown menu:

- **Above:** The trigger is activated if the value of the selected channel exceeds a defined value.
- **Below:** The trigger is activated if the value of the selected channel falls below a defined value.
- **Equal to:** The trigger is activated if the value of the selected channel is the same as a defined value.
- **Not Equal to:** The trigger is activated if the value of the selected channel is different than a defined value.

[value]

Define the value PRTG will compare the channel data to. Enter values in the smallest possible (base) unit, for example, in **bytes**, **milliseconds**, or **percent**. Please enter an integer value.

..for at least [...]
seconds

Define how many seconds PRTG waits before it sends out a notification (**latency**). This can avoid false alarms in case a channel reaches a limit for just a few moments. If the defined channel condition persists after the defined time span, the notification is triggered. Please enter an integer value.

 Do not define a latency that is shorter than the scanning interval of a sensor that uses this trigger! The notification trigger might not work as expected in this case.

THRESHOLD TRIGGER

...perform [...]	Select a notification that is triggered if the defined channel condition is true and the latency time defined has elapsed. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notification Templates settings. You can also choose no notification to only use other conditions for this trigger.
When condition clears perform [...]	Select a notification that is triggered if the defined channel condition is not true any more because the channel value has changed again. Choose a notification from the dropdown menu. The menu shows all notifications defined in the Account Settings—Notification Templates settings. You can also choose no notification to only use other conditions for this trigger.  PRTG sends notifications about cleared conditions if the time for the trigger activation elapsed (defined in the first line) and you choose a notification here. If you select no notification above, you will get the notification about the cleared condition nevertheless if you define it here.
Save	Click Save to confirm your settings.
Cancel	Click Cancel to undo your changes.

 No escalation notification and no repeat are available for this trigger type.

Add Change Trigger

Define a trigger that is activated by an 'on change' trigger. Some sensors offer the option to send such a trigger whenever sensor values have changed. Hover over  and select **Add Change Trigger** from the menu to add a new trigger, or click the **Edit** button next to an existing notification to change it. Then define settings as described below. Every trigger will provoke one or more [notification\(s\)](#) to be executed.

CHANGE TRIGGER

When sensor changes perform [...]

Select a notification that is triggered whenever a compatible sensor sends a 'change notification'. You can enable this option in the [settings](#) of some sensors. The notification trigger is activated immediately whenever a sensor sends an 'on change' trigger. Choose a notification from the dropdown menu. The menu shows all notifications defined in the [Account Settings—Notification Templates](#) settings.

 There are no other options available for this trigger type.

Sensor Settings Overview

For information about sensor settings, see the following sections:

- [Sensor Settings—List of Available Sensor Types](#)
- [Additional Sensor Types \(Custom Sensors\)](#)
- [Sensor Channels Settings](#)
- [Sensor Notification Triggers Settings](#)

Object Settings Overview

 For more general information about object settings, see section [Object Settings](#).

Part 8

Ajax Web Interface—Advanced Procedures

8 Ajax Web Interface—Advanced Procedures

The PRTG web interface is the feature complete access to PRTG Network Monitor via the web. Use the PRTG web interface as default interface to setup your monitoring and bring it to perfection.

Configure devices and sensors, set up notifications, review monitoring results, create reports, visualize your monitoring on dashboards, and use many more PRTG features to complete your monitoring.

The PRTG web interface is based on Asynchronous Java Script and XML (AJAX) and designed to optimally adjust to your systems by its **responsive design**. It shows all object setting dialogs as pop-up layers, so you never lose the current context. The web interface adjusts to the size of your screen, so you always get information displayed in an optimized way.

While you are [logged in](#)¹⁶⁶, the PRTG web interface continuously refreshes the data on the screen via AJAX calls and you always are up to date on the current monitoring results. You can [set](#)³³⁷⁶ the refresh interval and method individually.

Thanks to **Single Page Application (SPA)** technology, your system will stay highly performant because only single page elements are refreshed when necessary.

The following sections introduce more advanced procedures in the Ajax Graphical User Interface (GUI).

Ajax Web Interface—Advanced Procedures—Topics

- [Toplists](#)³¹⁸⁶
- [Arrange Objects](#)³¹⁹¹
- [Clone Object](#)³¹⁹³
- [Multi-Edit](#)³¹⁹⁷
- [Create Device Template](#)³²⁰³
- [Show Dependencies](#)³²⁰⁹
- [Geo Maps](#)³²¹¹
- [Notifications](#)³²¹⁶
- [Libraries](#)³²³⁵
- [Reports](#)³²⁵²
- [Maps](#)³²⁷⁸
- [Setup](#)³³⁰²

Other Ajax Web Interface Sections

- [Ajax Web Interface—Basic Procedures](#)¹⁶⁶

- [Ajax Web Interface—Device and Sensor Setup](#)  280

Related Topics

- [Enterprise Console](#)  3430
- [PRTG Apps for Mobile Network Monitoring](#)  3484

8.1 Toplists

Packet Sniffer and **xFlow** (NetFlow, jFlow, sFlow, IPFIX) sensor types can not only measure the total bandwidth usage, they can also break down the traffic by IP address, port, protocol, and other parameters. The results are shown in so-called **Toplists**. This way PRTG is able to tell which IP address, connection, or protocol uses the most bandwidth.

PRTG looks at all network packets (or streams) and collects the bandwidth information for all IPs, ports, and protocols. At the end of the toplist period, PRTG only stores the top entries of each list in its database.

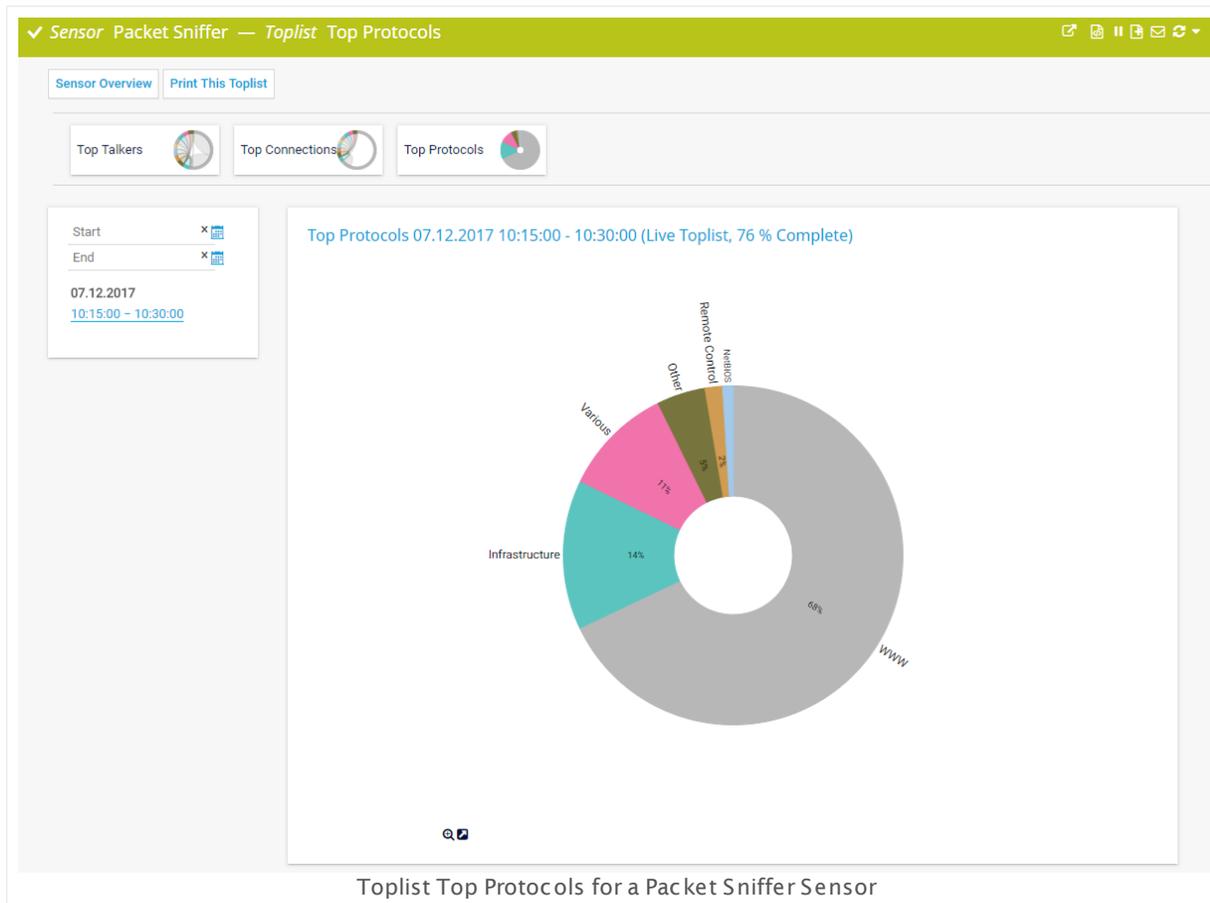
Only Top Entries are Stored

Storing all available analysis data in a database during the analysis process would create a huge amount of data, which would be very slow to transfer between probe and core and also retrieving data would be too slow. By storing only the top 100 entries for short periods of time it is possible to reduce the amount of data to a minimum while still being able to identify devices with huge bandwidth usage.

Toplists Overview

Toplists are available for [xFlow, IPFIX, and Packet Sniffer sensors](#)⁴³⁰ only. Toplist graphs are displayed right on the sensor overview page. By default, there are three different toplist predefined for each sensor:

- **Top Connections:** Shows bandwidth usage by connection.
- **Top Protocols:** Shows bandwidth usage by protocol.
- **Top Talkers:** Shows bandwidth usage by IP address.



- Click one of these items to view a distribution chart and a list of source and destination IP and port, protocols, kind of traffic in different channels, for example. What kind of information is available depends on the list selected.
- Click an entry in the Toplist periods list on the left side to view data for a certain time span. By default, a time span of 15 minutes is set. You can also manually define start and end time of the Toplist period you want to view. Use the date time picker to enter the date and time. Additionally, several [table list options](#)^[237] are available.
- To print a Toplist, click the **Print This Toplist** button to view a printer-friendly version. Use the print option of your browser to send it to your printer.
- With **Sensor Overview** you can return to the current sensor's **Overview** tab. For a quick selection of other Toplists of the current sensor, click one of the Toplist icons at the top of the page.
- You can add or delete new Toplists, or edit existing ones on the sensor's **Overview** tab,

Add

Click the **Add Toplist** button in the sensor overview to create a new Toplist. The available options are the same as for [editing](#)^[318] a list.

Edit

Click the small **gear icon** of a Toplist tile in the sensor overview to modify it.

TOPLIST	
Name	Enter a meaningful name to identify the toplist.
Type	<ul style="list-style-type: none"> ▪ Top Talkers (Which IPs use the most bandwidth?): Shows bandwidth usage by IP address. ▪ Top Connections (Which connections use most bandwidth?): Shows bandwidth usage by connection. ▪ Top Protocols (Which protocols use the most bandwidth?): Shows bandwidth usage by protocol. ▪ Custom (Create your own Toplist): Create your own list by selecting criteria below.
Toplist Fields	<p>This setting is only available if you select a custom type above. Select the fields you want to add to the Toplist by adding a check mark in front of the respective field name. The available options depend on the type of sensor used. They are different for Packet Sniffer, NetFlow v5, v9 (and IPFIX), and sFlow.</p> <p> For performance reasons, only select the fields you really want to monitor.</p> <p> For more information, see Performance Considerations  section below.</p>
Period (Minutes)	<p>Define the interval for the Toplist in minutes. Please enter an integer value. Toplists always cover a certain time span. Once a time span has passed, the top results are stored and a new Toplist is started.</p> <p> To avoid load problems on your probe system, please do not set this interval too long. Default setting is 15 minutes.</p> <p> For more information, see Performance Considerations  section below.</p>
Top Count	<p>Define the length of your Toplist. Only this number of entries will be stored for each period. Please enter an integer value.</p> <p> To avoid load problems on your probe system, please set this value as low as possible. Default setting is 100 to store the top 100 entries for each period.</p>

TOPLIST

 For more information, see [Performance Considerations](#)  section below.

Reverse DNS

Define if you want to do a reverse Domain Name Service (DNS) lookup for IP addresses stored in the Toplist. Choose between:

- **Do a reverse DNS lookup for IPs:** Determine the domain name associated with an IP address and show it in the Toplist.
- **Do no reverse DNS lookup (faster):** Show IP addresses only. Choose this option to increase performance.

Probe/Core Data Transfer

Define how the probe sends the Toplist data set to the core server. Choose between:

- **According to sensor interval (default):** Send data in the interval defined in the settings of the sensor for which you create this Toplist. This can create a lot of bandwidth and CPU load with many sniffer sensors, complex traffic, or long Toplists.
- **Wait until Toplist period ends (less CPU and bandwidth usage):** Send data once a Toplist period has finished. This will create less bandwidth usage and CPU load, but you cannot see the **current** Toplist in the web interface, only Toplists with finished periods.

 For more information, see [Performance Considerations](#)  section below.

Memory Limit (MB)

Define the maximal amount of memory in MB that the probe will use for collecting the different connection information. Every Toplist adds its amount to the probe's memory consumption. Increase this value if the number of captured connections is not sufficient. Please enter an integer value.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Delete

Click the small **trashcan icon** of a Toplist tile in the sensor overview to delete it. Confirm with **Delete** to delete the list.

Details

Click on the **windows symbol** to show details of a Toplist.

Performance Considerations

If you create Toplists for data lines with considerable usage (for example, steady bandwidth over 10 Mbit/s) or if the traffic is very diverse (for example, many IPs or ports with only little traffic each) please consider the following aspects:

- The probe gathers all information needed for the Toplist in RAM memory during each period. Only the top 100 entries are transferred to the core. Depending on the Toplist type and traffic patterns, the required memory can grow into many megabytes.
- Choose periods that are as short as possible (especially important when traffic has a high level of diversity) to minimize memory usage.
- Memory requirements can grow almost exponentially with each field used in the Toplist definition (depending on traffic pattern). Avoid complex Toplists for high and diverse traffic. For example, **Top Connections** (5 fields) needs a lot more memory than **Top Talkers** (1 field).
- If you experience high bandwidth usage between core and probe, try to choose the **Wait until Toplist period ends** option in the [Toplist settings](#)³¹⁸⁸.
- If you experience **Data incomplete, memory limit was exceeded** messages, try to increase the memory limit in the Toplist settings but keep an eye on the memory usage of the probe process.
- To increase the performance of a Toplist, disable the reverse DNS lookup.

Notes

- When working with Toplists, be aware that privacy issues can come up for certain configurations of this feature. Using Toplists you can track all single connections of an individual PC to the outside world and you, as the administrator, must make sure it is legal for you to configure PRTG like this.
- Keep in mind that Toplists can be viewed through the web interface. You may not want to show lists of domains used in your network to others, so restrict [access rights](#)¹⁵⁸ to sensor types having Toplists.
- Note that diagrams, for example, for top connections are not meant to be used for detailed analysis. Rather they should indicate if there is an uncommon bigger change in this Toplist.

More

- [Monitoring Bandwidth via Flows](#)³⁵¹⁴
- [Monitoring Bandwidth via Packet Sniffing](#)³⁵¹²

8.2 Arrange Objects

There are several options to move objects within the device tree, or to move objects from one probe or group to another.

Manage Tab in Device Tree

While viewing the device tree (or parts of it), click the **Management** tab to switch to a tree view where you can move monitoring objects using drag&drop in your browser window. For more information, see section [Manage Device Tree](#) [329].

Device Details View: Arrange Sensors

When you view the **Overview** tab of a device, you see a list of all sensors on this device.

The screenshot shows the 'Device Probe Device' overview page. At the top, there are navigation tabs for 'Overview', '2 days', '30 days', and '365 days'. Below this, there are sections for 'Status: OK', 'Sensors: 22 (of 28)', 'DNS/IP: 127.0.0.1', and 'Dependency: Ping'. A 'Graph' section shows four gauges for 'Core Health', 'Probe Health', 'System Health', and 'Ping', all at 100% health. Below the gauges is a table of sensors:

Pos	Sensor	Status	Message	Graph	Priority
1.	Core Health	Up	OK	Health 100%	★★★★★
2.	Probe Health	Up	OK	Health 100%	★★★★★
3.	System Health	Up	OK	Health 100%	★★★★★
4.	Disk Free	Up	OK	Free Space C: 70%	★★★☆☆
5.	Common SaaS Check	Up	OK	Available Sen. 100%	★★★☆☆
6.	Surface Ethernet Adapter	Up	OK	Total 179 kbit/s	★★★☆☆
7.	Sensor Factory	Up	OK	Local Probe 100%	★★★☆☆
8.	IPFIX	Unknown	No data since startup	Total No data	★★★☆☆

At the bottom of the screenshot, the text 'Arrange Sensors on a Device' is visible.

Click the column headers **Pos**, **Sensor**, **Status**, or **Priority** to re-sort the sensor list. To change a sensor's position, click the small grip at the beginning of the row, drag it to the position you like, and drop it. Changes take effect immediately.

Context Menu: Move

You can also right-click any object in the device tree to show the [context menu](#)²⁴⁷. Select the **Move** entry to move sensors, devices, or groups up and down, or to move groups or devices into other groups or on other probes.

8.3 Clone Object

If you want to duplicate an object with the same settings, you can clone it. Cloning is available for groups, devices, and sensors. Unlike the results when using the [Create Device Template](#) ³²⁰³ option, a cloned device contains all objects of the original device, regardless of whether they bring about working sensors or not. This often depends on the settings of the cloned device.

The new object takes over all settings of the original object. This means, for example, that an [Auto-Discovery](#) ²⁸²¹ will start automatically on a cloned device (as soon as you resume it) if this option is set on the original device.

To start, right-click an object in your device tree, and from the [context menu](#) ²⁴⁷¹, select **Clone...** to open an assistant.

Clone Sensor Business Process 1



Duplicating Sensor by Cloning

To duplicate a sensor by creating a clone of this sensor choose a parent device and a new name for the sensor.

Note: After creation the new sensor is paused so you can edit its settings before monitoring is actually started.

Sensor To Be Cloned

Parent Probe

Local Probe (Local Probe)

Parent Group

Local Probe (Local Probe)

Parent Device

Probe Device

Sensor

Business Process 1

Name for New Sensor

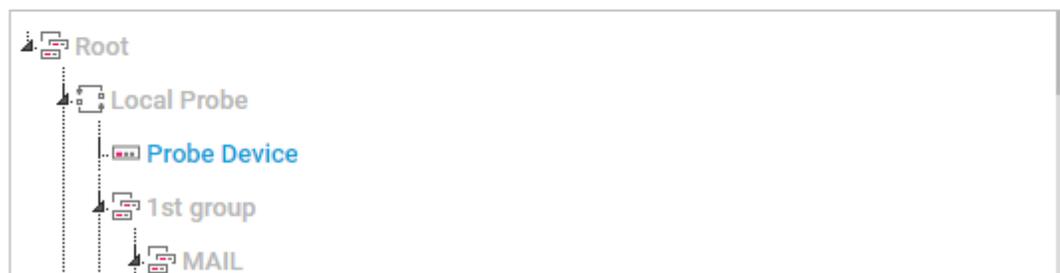
New Sensor Name

Clone of Business Process 1

Parent Device for New Sensor

Select a device to which you want to add the sensor clone.

Search...



[Cancel](#)

[Continue](#)

- ❗ You cannot clone **fixed** objects, such as the root group, a probe device, or PRTG system internal sensors.
- ❗ If you want to clone a **sensor**, a faster way is to use the [Manage Device Tree](#)^[329] function.
- ❗ The [user account](#)^[3376] that clones an object must have at least [read access](#)^[158] to this object and all objects underneath in the [hierarchy](#)^[133]. The user group of this account must have the [permission to create all sensor types](#)^[3384] that run on the device or group that is going to be cloned.

Clone Object Settings

OBJECT TO BE CLONED

Object Several fields show information about the object that you are cloning. The available information varies depending on whether you clone a group, device, or sensor.

NAME OF NEW OBJECT

New Object Name Enter a meaningful name for the new object to identify it later in, for example, the device tree or lists. By default, PRTG uses the old name with a preceding **Clone of**.

New IP Address/DNS Name This field is only available when you clone a device. Enter the IP address or DNS name for the new device.

Service URL This field is only available when you clone a device. Specify a URL you would like to open directly when you select **Device Tools | Go To Service URL** from the [context menu](#)^[254] of the device. For example, you can configure this option to call the address <http://www.example.com/service.html>. Enter a valid URL or leave the field empty.

PARENT GROUP/DEVICE FOR NEW OBJECT

Use the [object selector](#)^[240] to choose the object that you want to add the object clone to. If you clone a group or device, select a group. If you clone a sensor, select the device you want to add it to.

Save your settings. If you leave the current page, all changes to the settings will be lost!

✔ Results

- If you have cloned a sensor, the [overview](#)^[198] tab of the new sensor (the clone) will open.
- If you have cloned a group or device, you will stay on the current page.
- By default, all sensors are initially [paused](#)^[245] so you can change settings before monitoring starts. Please check the [settings](#)^[217] of the new objects and [resume](#)^[245] monitoring.

Related Topics

- [Create Device Template](#)^[320]
- [Manage Device Tree](#)^[329]

8.4 Multi-Edit

Device and sensor table lists, as well as some other lists, offer multi-edit functionality. With this, you can bulk edit the properties of many objects at a time. Multi-edit is also available in the **Management** tab if you select multiple objects by holding down the **Ctrl** key (see [Manage Device Tree](#)³³⁰).

- ❗ You cannot change every setting type with multi-edit. PRTG only displays settings that all selected objects have in common.
- ❗ You cannot multi-edit the standard [user groups](#)³³⁸ "PRTG Administrators" and "PRTG Users Group".

Ping Sensors

Items: 50
Show Filters

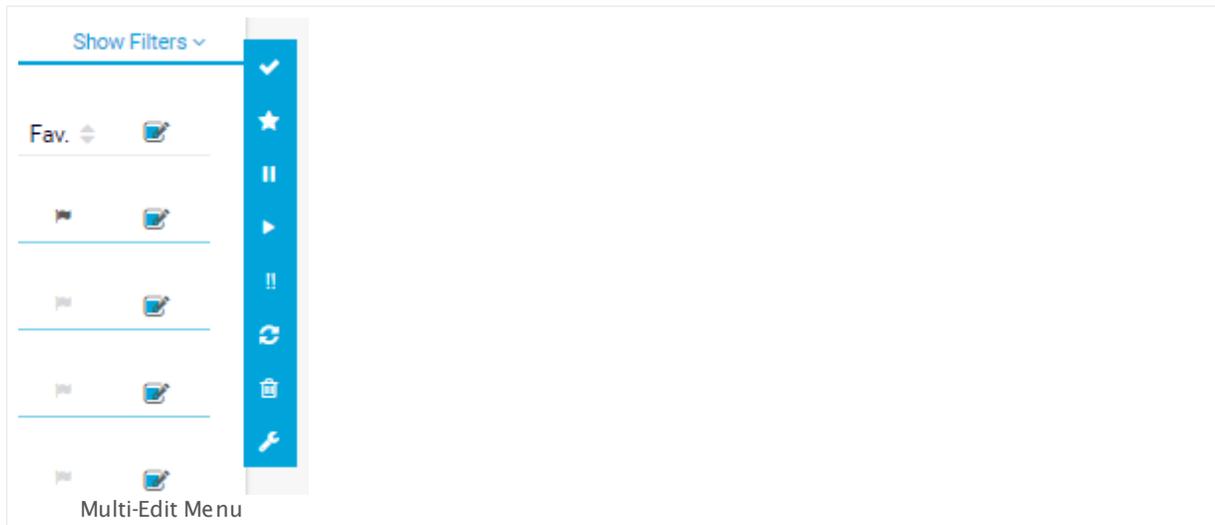
Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	1 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	1 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	1 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	1 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	0 msec	OK		★★★★★	🔖	
<input checked="" type="checkbox"/> PING		Up	1 msec	OK		★★★★★	🔖	

Example of a Table List

Start Multi-Edit in Lists

Start with viewing a table list. For example, choose **Sensors | By Type | ...** or **Devices | Device List | ...** from the [main menu bar](#)²⁶³. Table lists are also available in the **Overview** tab of [Libraries](#)³²³⁵, [Maps](#)³²⁷⁸, [Reports](#)³²⁵², [Notifications](#)³²¹⁶, and [Schedules](#)³³³⁸.

In a table list, start multi-edit by selecting objects using the check boxes on the right. You can also select all objects of the current page at once by clicking the check box in the table header. Use the **Items** option to view more items per page. As soon as you select one or more objects, the multi-edit menu appears at the top of the table. Chosen objects are marked by a blue line.



Depending on the object type, different functions are available. For example, for sensor lists, some frequently used functions are available as quick buttons, such as **Delete**, **Pause**, **Resume**, **Scan Now**, and **Settings**. Click one of the buttons to apply the respective function to all selected objects.

The options in this menu vary depending on the kind of objects selected. Choose an entry to apply the according function to all selected objects.

Once you have selected the objects you want to change settings for, click the wrench symbol to enter the edit settings mode. For available settings, see below.

Start Multi-Edit in Management Tab

In the device tree, start by clicking the **Management** tab.

You can use Multi-Edit for object settings:

- Hold down the **Ctrl** key and select multiple groups, devices, or sensors (one of a kind).
- In the appearing dialog, select the settings you want to edit, change the according values, and click **Save**. The changes will be applied to all selected objects.

For available settings, see below.

Edit Settings—Settings

The **Edit Multiple Objects** dialog box shows most of the settings that the selected sensors respective devices have in common. For example, you can edit the name, tags, priority, scanning interval, and access rights.

To change a property, add a check mark in front of the respective line and then change the settings. The new setting(s) will be applied to all objects you selected for multi-edit. All properties that are not activated with a check mark remain unchanged.

Click **OK** to store your settings. If you close the dialog box via the **X**, all changes to the settings will be lost!

Edit Settings—Channel Settings

The **Channel Settings** tab in the **Edit Multiple Objects** dialog box is only available when editing sensors. You can edit settings of all channels that the selected sensors have in common. Select a channel name from the **Channel** list. You can then edit display settings, colors, scaling, and limits, for example.

Editing 2 Objects
✕

Edit Multiple Objects

This page allows to edit one or more settings for a selection of objects (groups, devices, sensors, etc.). First enable the checkbox in the first column for each setting that you want to change for all selected objects. Then enter/select your new value.

You are editing 2 objects (Show all objects):

⚙ Settings
⚙ Channel Settings

Select Channel

Channel

- Downtime (ID -4)
- Ping Time (ID 0)
- Minimum (ID 1)
- Maximum (ID 2)
- Packet Loss (ID 3)

Edit Channel ""

- Graph Rendering** ⓘ
 - Show in Graphs
 - Hide from Graphs
- Table Rendering** ⓘ
 - Show in Tables
 - Hide from Tables
- Line Color** ⓘ
 - Automatic
 - Manual
- Line Width** ⓘ
 - 1

Cancel OK

Example of Sensor Channel Settings in Multi-Edit Mode

The available options depend on the selected sensors and vary according to your selection. It may be useful to only choose one certain sensor type from the list, so that there are as many channel settings as possible available for multi-edit.

To change a property, add a check mark in front of the respective line and then change the channel settings. The new setting(s) will be applied to all sensors you selected for multi-edit. All properties that are not activated with a check mark remain unchanged.

Click **OK** to store your settings. If you close the dialog box via the **X**, all changes to the settings will be lost!

Related Topics

- [Working with Table Lists](#) 
- [Manage Device Tree](#) 

8.5 Create Device Template

If you want to add a certain device several times, you can create a device template from an existing device in your device tree. When creating a device template, PRTG will save information for nearly all sensors on this device to a template file that you can later use in combination with [Auto-Discovery](#)^[282] ([restrictions](#)^[3205] apply for a few sensor types). There are also custom device templates available in the [PRTG Script World](#).

From the sensors, all relevant settings are saved, except settings that refer to other objects, such as [schedules](#)^[142], [notification triggers](#)^[3216], and [access rights](#)^[158]. PRTG will automatically revert them to **Inherit**.

To start, right-click a device in your device tree. From the [context menu](#)^[247], select **Create Device Template...** An assistant appears.

Create Device Template for Probe Device
✕

Creating Device Templates

To create a template that you can use for auto-discovery you have to provide a file name and a clear text name. PRTG uses the clear name in the select box for device templates in the auto-discovery assistant. A template contains an entry for every sensor of the selected device. This entry contains all relevant sensor settings except settings that refer to other objects like schedules, triggers, access rights. These settings will revert to 'inherited' when you create a sensor via a template.

Note: There are sensor types that you cannot save into a device template. For a list of these sensor types, see [PRTG Manual: Create Device Template](#)

Choose Template Name

File Name [?]

This field is required.

Template Name [?]

This field is required.

You can exclude sensors from the template by setting the check mark in the list below.

Note: Sensors that cannot be saved into device templates do not appear in this list.

Note: Sensor types that dynamically scan for available monitoring items when you add the sensor to a device do not appear in this list. PRTG includes these sensors automatically into the template if they support template functionality and you cannot exclude them.

Exclude Sensors

Q

Sensors

<input type="checkbox"/>	<input checked="" type="checkbox"/> Common SaaS Check
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disk Free_Local
<input type="checkbox"/>	<input checked="" type="checkbox"/> Free Disk Space (Multi Drive) 3
<input type="checkbox"/>	<input checked="" type="checkbox"/> HTTP Data Advanced 2
<input type="checkbox"/>	<input type="checkbox"/> ...

Cancel
Continue >

Create Device Template Assistant

i Device templates only save the sensors on the device and the sensors' settings, including channels. The device itself and its settings are not saved. For successful device template creation, sensors must be added to the device (either [manually](#)^[325] or via [Auto-Discovery](#)^[282]) and must be [device template-capable](#)^[326].

Device Template Settings

CHOOSE TEMPLATE NAME

File Name	<p>Enter a name under which PRTG will store the file. Template files have the extension .odt in the \PRTG Network Monitor \devicetemplates sub-directory of your PRTG core installation ³⁷³⁴ (of the Master node, if in a cluster ^{130b}). If a file with this name already exists in this directory, you will see an according error message.</p> <p> The device templates folder is not accessible on PRTG hosted by Paessler.</p>
Template Name	Enter a meaningful display name for the template as it will appear in the web interface.
Exclude Sensors	<p>Select sensors that you do not want to include into the device template. Mark the corresponding check boxes of the sensors that you do not want to include into the device template.</p> <p> Sensors that cannot be saved into templates ³²⁰⁵ will not appear in this list.</p> <p> Sensor types that dynamically scan for available monitoring items when you add the sensor to a device will not appear in this list. PRTG includes these sensors automatically into the template if they support template functionality. You cannot exclude them from the device template that you create.</p>

Save your settings. If you leave the current page, all changes to the settings will be lost!

If your template file was saved successfully, you will see an according message and can review the sensors that were added. Click **OK** to finish. The device template is now stored in the program path of your PRTG core installation. Your device template file contains all sensors, including their settings, of the original device.

During your next auto-discovery, choose the **Automatic sensor creation using specific device template(s)** option and select the name of your newly created device template from the list. PRTG will then try to discover the stored sensor types on the new (or existing) device. If the physical device answers to a sensor request, the sensor is added to the PRTG device.

 For detailed information, see section [Auto-Discovery](#) ²⁸².

Settings That Are Not Saved

There are a few settings that you cannot save into a device template, so PRTG will set them to default, for example:

- the **Dependency Type** setting **Master object for parent** (in **Schedules and Dependencies** section)
- **Result Handling** setting **Write result to disk** because this is intended for debugging purposes only.
- Settings in the **Access Rights** section are not saved to avoid security flaws.

i In general, you cannot save all [Sensor Settings](#)^[428] and [Sensor Channels Settings](#)^[3160] (for example, channel limits) of sensor types that dynamically scan for available monitoring items when you add the sensor. This affects, for example, **traffic sensors** where you can choose interfaces that you want to monitor in the [Add Sensor](#)^[325] [dialog](#)^[325].

Furthermore, due to internal restrictions, the following sensor types will not be saved into a device template:

- **Amazon CloudWatch sensors**
- **Business Process**
- **Core/Probe/Cluster Health**
- **DHCP**
- **DICOM Bandwidth**
- **DICOM C-ECHO**
- **DICOM Query/Retrieve**
- **Docker Container Status**
- **Dropbox**
- **Enterprise Virtual Array**
- **Exchange Backup (PowerShell)**
- **Exchange Database (PowerShell)**
- **Exchange Database DAG (PowerShell)**
- **Exchange Mail Queue (PowerShell)**
- **Exchange Mailbox (PowerShell)**
- **Exchange Public Folder (PowerShell)**
- **Google Analytics**
- **Google Drive**
- **HL7**
- **IPFIX**
- **IPFIX (Custom)**
- **IPMI System Health**
- **jFlow V5**
- **jFlow V5 (Custom)**

- **Microsoft OneDrive**
- **NetApp Aggregate**
- **NetApp I/O**
- **NetApp LIF**
- **NetApp LUN**
- **NetApp NIC**
- **NetApp Physical Disk**
- **NetApp SnapMirror**
- **NetApp System Health**
- **NetApp Volume**
- **NetFlow V5**
- **NetFlow V5 (Custom)**
- **NetFlow V9**
- **NetFlow V9 (Custom)**
- **Packet Sniffer**
- **Packet Sniffer (Custom)**
- **Passive Application Performance**
- **QoS (Quality of Service)**
- **QoS (Quality of Service) Roundtrip**
- **REST Custom**
- **REST Dell EMC Capacity**
- **REST Dell EMC File System**
- **REST Dell EMC LUN**
- **REST Dell EMC Pool**
- **REST Dell EMC System Health**
- **Sensor Factory**
- **sFlow**
- **sFlow (Custom)**
- **SNMP Trap Receiver**
- **Syslog Receiver**
- **WMI Security Center**

No Update of Device Templates

Once a device template is created, it is not possible to add additional sensors to it via the PRTG web interface. If you want to create a template with an extended set of sensors, please create a new one.

 When saving a new device template, all internal IDs of the sensors in this template are updated. Because of this, when you apply a new template to an existing device, PRTG will newly create all sensors that this template contains on this device, even if these sensors were previously created using another device template!

 You cannot directly delete device templates.

 You cannot edit existing template files on PRTG hosted by Paessler.

Related Topics

- [Clone Object](#)  3193
- [Manage Device Tree](#)  329

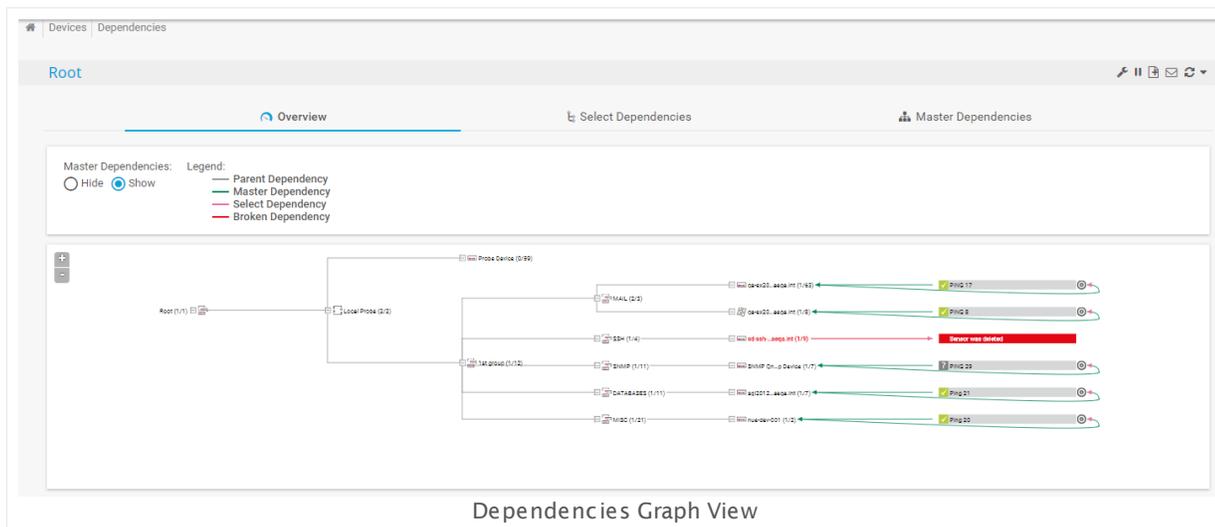
8.6 Show Dependencies

This function shows an overview of the dependencies configured for the objects in your setup.

For a general introduction, see the [Dependencies](#) section.

In the [main menu bar](#), hover over **Devices | Dependencies** to show other menu items. Follow the menu path (it is specific to your setup) to view dependencies of the objects in a specific probe or group only.

- **Selected Dependencies** shows a table of manually set dependencies (section [Select object](#) in any object's settings).
- **Master Dependencies** shows a table of master dependencies.
- **Dependencies Graph** shows a visualization of device, group, and sensor dependencies. See [below](#).



Dependencies Graph

Click **Dependencies Graph** to see the device tree in the dependencies graph view with lines of different color connecting objects. Hover over **Dependencies Graph** to show other menu items for the dependency graph (probes and groups). Click a probe or group menu item to show its dependencies directly. The lines in the dependencies graph symbolize dependencies between the monitoring objects in the device tree. Additionally, a [color code](#) is used for the dependencies.

To show the Dependencies Graph, you need to access the PRTG web interface as a **PRTG System Administrator** user.

- Above the graph header bar, you can switch the dependencies view to tables of the currently selected object with the **Select Dependencies Table** and **Master Dependencies Table** tabs. The **Overview tab** shows an overview of the currently selected object.

- Mark the radio buttons in the header bar to **Show** or **Hide** master dependencies. By default, **Hide** is selected and only **parent**, **selected**, and **broken** dependencies are shown.
 - ❗ These buttons are not available in Internet Explorer for technical reasons. Please use Google Chrome 67 or later (recommended) or Mozilla Firefox 61 or later.
- Click the **+** or **—** buttons on the left in the header bar to zoom in or out of the graph.
- Click probe and group nodes to show the respective dependencies.
- Click device or sensor nodes to open the corresponding overview tab.
- Click the **+** or **—** boxes to expand or collapse probe and group nodes.
- Numbers in parentheses indicate how many child nodes of an object are shown.

Color Code of Dependencies Graph

The line's colors show the kind and source of a dependency. This represents the **Dependency Type** as defined in the **Schedule, Dependencies, and Maintenance Window** [settings of a probe, group, device, or sensor](#)^[280].

- ❗ You can find the color legend also in the graph header bar.
- **Gray**
Gray lines show a dependency by inheritance (**Use parent**). The source of the dependency is the parent object on the left end of the line, for example, **Root** is the parent of **Local Probe**.
- **Green**
Green lines show a master dependency for a device (**Master object for parent**). The sensor that is set as the master points to the dependent device with a green arrow head at the line's end. The arrow head from the dependent device to its master object is pink.
- **Pink**
Pink lines show a dependency that was set manually (**Select object**). The source of the dependency points to the dependant with a pink arrow at the line's end.
- **Red**
Red lines indicate broken dependencies, for example, if the master is not available.

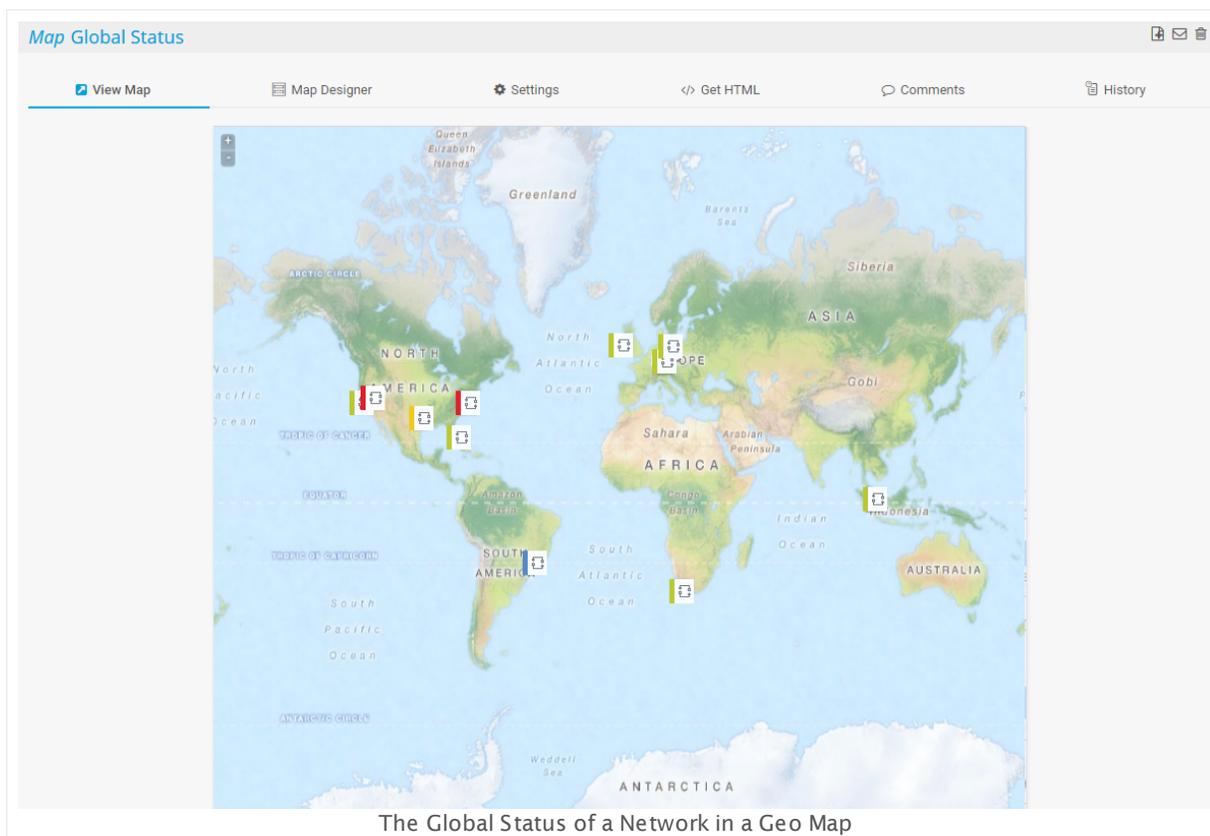
8.7 Geo Maps

With the PRTG Geo Maps feature you can visualize geographical information about your monitored objects. You can display the location of **probes**, **groups**, and **devices** in a graphical map on the details page of an object, or on PRTG [Maps](#)^[3276]. This feature is especially useful when you monitor networks that are spread over several different locations. Devices located in a few cities of a country or various continents can all easily be visualized.

You can enter **Location** information for each probe, group, and device. PRTG uses the first line of this information to query a geographical map that shows your objects. Your location specification is resolved to global geographical coordinates by the PRTG core server with the help of an external map service provider.

PRTG connects to the specified maps provider to get **map tiles**. The map tiles provide the (geo) graphical "background". Then PRTG marks the defined locations with the corresponding object icons and their **status**^[3213] on the map. You can select your favorite map tiles provider in [System Administration—User Interface](#)^[3346] (setting **Geo Maps**).

You can display geographical maps on the device tree. PRTG adjusts the zoom of a map automatically so that it can show all locations of a selected object. You can also add geographical maps to PRTG [Maps](#)^[3276]. To do so, open the PRTG [Map Designer](#)^[3267] (either in an existing map or create a new one) and click **Geo Maps** in the properties menu on the right.



Using Geo Maps

To use geographical maps within the PRTG [web interface](#)^[166] or [Enterprise Console](#)^[3430], please ensure the following:

1. In the system administration in the PRTG web interface, select the maps provider and type you want to view. There, you will also find an option to disable geo maps integration if you do not want to use it. See section [System Administration—User Interface](#)^[3346] (setting **Geo Maps**) for detailed information.
2. In the [settings of a monitoring object](#)^[217] (probe, group, device), add a city name, address, or coordinates in the first line of the **Location** field. When you view the details of this object, PRTG will show a geographical map. PRTG uses the **Location** information also when you view objects in the [Enterprise Console](#)^[3430] or add **Geo Maps** objects to PRTG [Maps](#)^[3276].
3. Make sure your PRTG core server has access to the internet to obtain map tiles. If a proxy is mandatory in your network, configure proxy settings accordingly.
 -  For details, see [System Administration—Core & Probes](#)^[3368].
 -  For details about tile server domains, see this Knowledge Base article: [Which domains and ports does the GeoMaps feature use?](#)

Labeling Locations

You can define your own labels for locations of objects. To do so, enter the desired label in the first line of the **Location** settings and provide the geo coordinates of the location in the second line. This object will appear with the defined label in PRTG geo maps.

For example, add the following to the location field:

```
Big Apple
40.712778,-74.005833
```

Location

 inherit from

Location (for Geo Maps) ⓘ

```
Big Apple
40.712778,-74.005833
```



Defining Location New York City with Geo Coordinates and Label Big Apple

The location New York City appears with the label Big Apple:

Geo Map for Root

Big Apple

Device	!!	!!	!	✓	W	II
SSH	13			15		
avocado	12			2	1	
DNS/ADS	4			38		
Cluster Probe Device	3			14	1	
DHCP	3			15	1	
Exchange	2			3	2	
Gateway	2			2		
Probe Device	2			10	1	

Location New York City with Label Big Apple

It is also possible to define the same label for different locations. For example, imagine your company's headquarter is spread over several different locations. For each object representing a dedicated headquarter in the PRTG device tree, enter its coordinates in the second line of the respective **Location** settings and the label "Headquarter" in the first line. All corresponding objects will be displayed as "Headquarter".

This way, you can easily find your desired objects on the map.

Map Icon Colors

On the geographical maps the different location icons show the overall [status](#) at this location by using a color code. Following, you can see all possible location states in order of their hierarchy:

Flag	Flag Color	Location Status	Meaning
	Red	Down	At least one sensor at this location shows a red Down status. Hover the circle with the letter symbol in the legend to view the total number of alarms at this location.
	Bright-Red	Down (Acknowledged)	At least one sensor at this location is Down and a PRTG user acknowledged this status with the Acknowledge Alarm function. The Down states of all sensors at this location must be acknowledged—if at least one sensor is unacknowledged down, this location will be displayed as Down .
	Yellow	Warning	At least one sensor at this location shows a yellow Warning status. There is no sensor in a Down or Down (Acknowledged) status at this location.
	Orange	Unusual	At least one sensor at this location shows an orange Unusual status. There is no sensor in a Down , Down (Acknowledged) , or Warning status at this location.
	Green	Up	All sensors at this location are in a green Up status. There is no sensor in a Down , Down (Acknowledged) , Warning , Paused , or Unusual status at this location.
	Blue	Paused	All sensors at this location show a blue Paused status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , or Up status at this location.
	Black (Grey)	Unknown	All sensors at this location have an Unknown status. There is no sensor in a Down , Down (Acknowledged) , Warning , Unusual , Paused , or Up status at this location.

 For detailed information about sensor states, see the section [Sensor States](#) ¹⁹⁵.

Geo Tracking of Your Mobile Device

It is possible to show the location of an Android device and track its movements on PRTG Geo Maps. PRTG can draw the route a device has taken directly into geo maps. For this feature, you need the [PRTG Mobile Probe for Android](#).

 For details, see this Knowledge Base article: [How can I track geo data of my Mobile Probe device?](#)

More

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- <https://kb.paessler.com/en/topic/34603>

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- <https://kb.paessler.com/en/topic/35823>

Knowledge Base: Why does my street not appear on the Geo Map shown in PRTG?

- <https://kb.paessler.com/en/topic/35653>

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- <https://kb.paessler.com/en/topic/32363>

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

- <https://kb.paessler.com/en/topic/7913>

Knowledge Base: How can I change the way markers look like in PRTG's geo maps?

- <https://kb.paessler.com/en/topic/43153>

Knowledge Base: How can I track geo data of my Mobile Probe device?

- <https://kb.paessler.com/en/topic/59647>

Knowledge Base: My geo maps are displayed without background. What can I do?

- <https://kb.paessler.com/en/topic/63608>

8.8 Notifications

PRTG uses notifications to send you alerts whenever PRTG discovers a defined status, such as slow or failing sensors, or when sensor channels breach threshold values. You can define an unlimited number of notifications allowing to use one, or more, of several communication channels like [email](#)³³¹⁷, [text messaging](#)³³²⁰, [push notifications](#)³³¹⁹ to Android and iOS devices, and [many more](#)³³¹⁶. PRTG sends notifications to the desired user's [Notification Contacts](#)³³³⁴ that you can define for each user account of your PRTG installation.

 See also our video tutorials for notifications:

- [Video Tutorial: Use Cases for Notifications](#)
- [Video Tutorial: How to Set Up and Use Notifications in PRTG](#)

Overview

PRTG sends a notification when a defined event evokes it. The following events can trigger notifications:

- **Sensor status changes**
For example, when a sensor changes its status from **Up** to **Down** or **Warning**, because responses are slow, or when a sensor status changes to **Unusual**.
- **Sensor value threshold breaches**
For example, when a sensor shows a request time higher than 1,000 ms for more than 30 minutes, or when free disk space is below 10%.
- **Speed threshold breaches**
For example, when a traffic sensor shows more than 1 Mbit/s for more than 5 minutes.
- **Volume threshold breaches**
For example, when a traffic sensor shows more than 1 Gbyte transferred in 24 hours.
- **Sensor value changes**
For some sensors you can trigger a notification whenever the value changes, for example, when monitoring files on a hard disk drive.

A notification can be one of these actions:

- [Send Email](#)³³¹⁷
- [Send Push Notification](#)³³¹⁹
- [Send SMS/Pager Message](#)³³²⁰
- [Send Slack Message](#)³³²¹
- [Send Microsoft Teams Message](#)³³²³
- [Add Entry to Event Log](#)³³²⁵
- [Send Syslog Message](#)³³²⁶
- [Send SNMP Trap](#)³³²⁷
- [Execute HTTP Action](#)³³²⁷
- [Execute Program](#)³³²⁸

- [Send Amazon Simple Notification Service \(SNS\) Message](#)  3329
- [Assign Ticket](#)  3331

 For details, see section [Account Settings—Notification Templates](#)  3316.

 Usually there are three successive attempts to deliver a notification. If all of these attempts fail, the notification is lost. To never miss a notification, we recommend that you always add two different ways to get a notification. For example, use the latency setting of a [state trigger](#)  3172 to choose a notification with another delivery method than in the first trigger condition, or set up a second trigger with another notification for the corresponding object.

Notifications can contain valuable sensor information, such as:

- Last error message
- Last good/failed request
- Total downtime
- Total uptime
- Recent sensor history
- A direct link to the web interface

 For available placeholders, see this Knowledge Base article: [What placeholders can I use with PRTG?](#)

Notifications Setup

Overall, you have to go through four steps to use notifications with PRTG. Please go through all of them for a first setup:

1. Check and set up the **Notification Delivery** settings if you use PRTG on premises. These define how PRTG will send messages.
 For detailed information, see [System Administration—Notification Delivery](#)  3361.
2. Check and set up **Notification Contacts** for the users of your PRTG installation. These define where to send notifications.
 For detailed information, see [Account Settings—Notification Contacts](#)  3334.
3. Check and set up several **Notification Templates**. These define the kind of message and its content.
 For detailed information, see [Account Settings—Notification Templates](#)  3311.
4. Check and set up **Notification Triggers** for objects. These provoke the defined notifications.
 For detailed information, see [Sensor Notification Triggers Settings](#)  3170.

 We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one [email notification](#)³³¹⁷ and one [SMS notification](#)³³²⁰. If delivery via email fails (due to a email server outage or for other reasons), PRTG can still notify you via your smartphone in this case as a fallback. You can achieve this, for example, by using the latency setting in a [state trigger](#)³¹⁷² and selecting a notification with another delivery method than for the first trigger condition.

 See the sections [Setting Up Notifications Based on Sensor Limits: Example](#)³²¹⁹ and [Setting up Notifications Based on Libraries: Example](#)³²²⁹ for a step-by-step guide that describes a potential notifications setup.

 There are also custom notification scripts available in the [PRTG Script World](#).

More

Video Tutorial: Use Cases for Notifications

- <https://www.paessler.com/learn/videos/prtg-basics/notifications-use-cases>

Video Tutorial: How to Set Up and Use Notifications in PRTG

- <https://www.paessler.com/support/videos/prtg-basics/notifications>

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

Knowledge Base: Notifications based on priorities

- <https://kb.paessler.com/en/topic/31243>

8.8.1 Setting up Notifications Based on Sensor Limits: Example

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

This section shows you exemplarily how to set up a notification for exceeded disk free limits. We provide the approach for this specific use case step by step so you can adapt it to define limits and corresponding notifications for other sensor types.

You have to take several steps to set up notifications based on limits:

- [Step 1:](#)³²¹⁹ Provide necessary information about the delivery of notifications (SMTP and SMS).
- [Step 2:](#)³²¹⁹ Specify recipients for notifications for each user account of your PRTG installation.
- [Step 3:](#)³²²⁰ Create notifications, specifying the type of notification and its content.
- [Step 4:](#)³²²¹ Define thresholds that change a sensor's status (this is not necessary for every kind of notification).
- [Step 5:](#)³²²⁵ Add suitable triggers to objects that evoke notifications if something is going wrong in your network.
- [Step 6:](#)³²²⁶ Test if the created notification is triggered and delivered correctly.

 When you set up your own notifications, you do not necessarily need to go through all the steps we describe here. In this section, our main goal is to give you a general idea of the notifications concept.

Step 1: Setting up the Notification Delivery

Before creating your actual notifications, you first have to define how those notifications are delivered to your email account, mobile phone, or pager. To do so, select **Set up | System Administration | Notification Delivery** from the PRTG main menu bar. Specify the mechanism of SMTP delivery, sender email and name, as well as the HELO ident. For SMS delivery, select your service provider and provide the corresponding credentials.

 You can find details about notification delivery in section [System Administration—Notification Delivery](#)³³⁶¹.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

Step 2: Setting up Notification Contacts

Create notification contacts to define where you want to receive notifications. Recipients can be email addresses, phone numbers (PRTG on premises only), or push devices (Android or iOS devices with the corresponding [PRTG smartphone app](#)³⁴⁸⁹). You can define as many recipients as you want for each user account in your PRTG installation. By default, the recipient "Primary Email Address" is available—this is the email address you provide in [your account settings](#)³³⁰⁴. This is sufficient for a first setup of notifications. Later on, when you see how it works, you can define more contacts. When you add a notification to a device, you just have to select a user or user group as recipient and PRTG uses the according contacts you define here.

 For details, see section [Account Settings—Notification Contacts](#)³³³⁴.

Step 3: Setting up the Notification's Content

To get an informative message when a disk is running out of capacity, create a corresponding notification. Select **Setup | Account Settings | Notification Templates** from the PRTG main menu bar, hover over  and click **Add Notification Template** from the menu. Give the notification an explanatory name; in our case you could use **Disk Free Limit Notification**. However, if you want to trigger this notification on a global level (for example, for a probe or group) such that it would not only apply to breached disk free limits, a general name would be more suitable (like the predefined notification "Email to Admin"). If you leave the default text of the newly created notification, it already contains all necessary information, for example:

- which sensor is affected,
- since when the sensor is affected,
- last value of this sensor.

 See section [More](#)³²²⁷ for the other options you have here.

After providing this basic information, select the delivery method. In our case, we choose **Send Email** for this notification by marking the corresponding check box. Specify who will receive the notification (select a specific user, for example, and PRTG sends the notification to all contacts of this user you specified in [step 2](#)³²¹⁹), its subject, the format, and its priority. By default, the email notification contains several information parameters about the evoking sensor: its name, status, time, message, location in the device tree, etc.

 You can choose any other notification method, of course. For more information, see [Account Settings—Notification Templates](#)³³¹⁶.

Send Email

Sender ? Default
 Custom

The three recipient settings below (user, user group, email address) work independently. So every contact and address selected by any of these settings will receive the notification.

Send to User ? ▼

Send to User Group ? ▼

Send to Email Address ?

Subject ?

Format ? HTML
 Text
 Text with custom content

Priority ? ▼

Creating an Email Notification

Once you set up the notification completely, click **Save**. PRTG opens the notifications overview page again. You can now use this notification for every trigger on every object in your device tree.

Step 4: Define Limits

Before creating triggers that evoke notifications, first specify the limits that you want to apply to your disks. For example, if you want to get a notification when a disk has exceeded 80% of its capacity, force the sensor into a **Warning** status at this utilization. You have several options to set limits for disk free sensors:

- Set limits checked against all disks in the settings of multi-drive sensors: [WMI Free Disk Space](#)²⁸³³, [SNMP Linux Disk Free](#)²²⁵¹, [SSH Disk Free](#)²⁵⁰⁷
- Enable limits in [Sensor Channels Settings](#)³¹⁶⁰ of single sensors.
- You can achieve both with [Multi-Edit](#)³¹⁹⁷.

Step 4.1: Define Limits in Sensor Settings (Multi-Disk Free Sensors Only)

You can set limits for sensors monitoring multiple disks directly via the **Settings** tab on a sensor's details page. [Multi-Edit](#)³¹⁹⁸ for existing sensors is also possible. Open the settings of the selected sensor(s) and go to section **Set limits checked against ALL disks**. There, for example, enable **Percentage Limit Check**. In the field **Lower Warning Limit**, enter the percentage that suits your needs. In our example, this would be **20**. Alternatively, you can use bytes to define a limit. However, we recommend using percentage values for more flexibility. This limit applies to all channels of this sensor that represent disks.

Editing 2 Objects
✕

Set limits checked against ALL disks

Percentage Limit Check ⓘ

Only use the limits in the settings of the percentage channels
 Use the limits of both the sensor and the channel settings

Upper Error Limit ⓘ

Upper Warning Limit ⓘ

Lower Warning Limit ⓘ

20

Lower Error Limit ⓘ

Alarm on Missing/Removed Disk ⓘ

Deactivate alarm (default)
 Activate alarm

Sensor Display

Graph Type ⓘ

Show channels independently (default)
 Stack channels on top of each other

Stack Unit ⓘ

%
 MByte

Cancel
OK

Setting Limits for All Disks

ⓘ This sensor setting is only available for multi-drive sensors. You can omit step 4.1 for all sensors that are not of the type "disk free".

Step 4.2: Define Limits for Sensor Channels

To set specific limits for single disks, use the sensor's **Channel** settings. You can open channel settings via the gear icon in the respective channel gauge or in the channels table. **Enable Limits** at the bottom of the channel settings dialog and specify your desired limits in the **Lower Warning Limit** field. This limit only applies to the respective channel.

i If you define channel limits when using the sensor's limit setting in the sensor's **Settings** tab at the same time, the first limit that applies will be considered. This way, you can individually define harder limits for single disks in a multi-disk sensor. All defined limits are valid side by side.

You **have** to take the approach via channel settings for sensor types that monitor only one (logical) disk, for example, the [SNMP Disk Free Sensor](#)²⁰⁶³. For these sensor types, you can use [Multi-Edit](#)³²⁰⁰ if you want to apply the same limits for each of these sensors automatically.

- To see all sensors of this type at a glance, just filter for it: From the main menu bar, select **Sensors | By Type | SNMP Disk Free**.
- Mark the check boxes of the sensors you want to add a limit for.
- Click the wrench symbol in the menu.
- Open the **Channel Settings** tab.
- Select the channel you want to add a limit for; in this case it would be most likely the channel **Free Space**.
- Then **Enable Limits** at the bottom of the dialog and enter the number in the correct field as described above.

When you are done, save these settings—the new limit applies to all channels with this name of the multi-edited sensors.

Editing 3 Objects x

Edit Channel

Limits ⓘ
 Disable limits
 Enable alerting based on limits

Upper Error Limit (%) ⓘ

Upper Warning Limit (%) ⓘ

Lower Warning Limit (%) ⓘ
20

Lower Error Limit (%) ⓘ

Error Limit Message ⓘ

Warning Limit Message ⓘ

Graph Rendering ⓘ
 Show in Graphs
 Hide from Graphs

Table Rendering ⓘ
 Show in Tables
 Hide from Tables

Line Color ⓘ
 Automatic
 Manual

Line Width ⓘ

[Cancel](#)

Setting Limits for Channels with Multi-Edit

Step 5: Setting up the Notification Trigger

You specified limits to define when a sensor will go into a **Warning** (or **Error**) status. Now you can create the according notification triggers. The notification trigger we use in this example is the **State Trigger**.

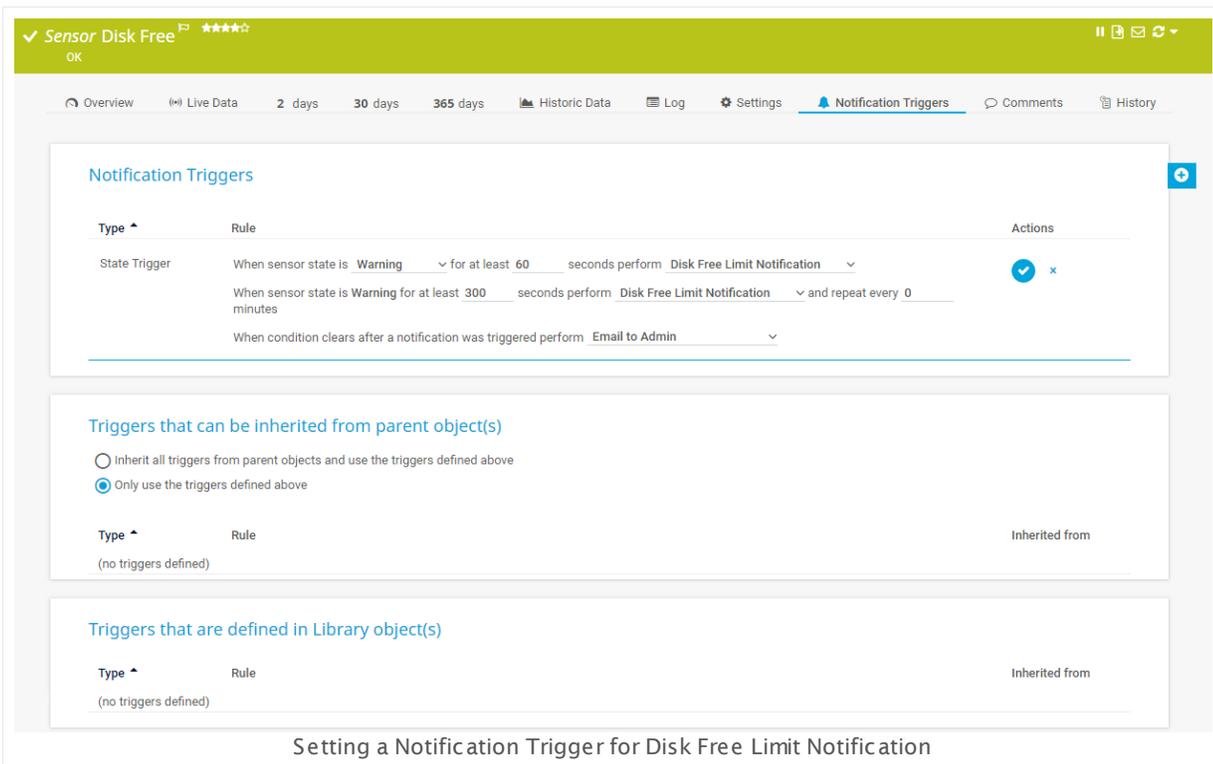
Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications

1 Setting up Notifications Based on Sensor Limits: Example

 For details about other possible notification triggers, see section [More](#)³²²⁷.

- You can set up a **State Trigger** on any level in your device tree. For example, open a group containing the device(s) representing your disks.
- Open the **Notification Triggers** tab.
- Hover over  and select a notification trigger from the menu.
- Set the notification trigger to "When sensor is Warning" and choose the notification template you created before ("Disk Free Limit Notification" or a more general one) from the dropdown list.
- Adjust the other notification trigger settings to your needs and save this new notification trigger.

Now you receive a notification immediately when the capacity of one of your disks falls below the defined limit, in this case 20% free disk space.



The screenshot shows the 'Notification Triggers' configuration page for the 'Sensor Disk Free' sensor. The interface includes a navigation bar with tabs for Overview, Live Data, 2 days, 30 days, 365 days, Historic Data, Log, Settings, Notification Triggers (active), Comments, and History. The main content area is titled 'Notification Triggers' and contains a table with columns for Type, Rule, and Actions. The table lists three triggers:

Type	Rule	Actions
State Trigger	When sensor state is Warning for at least 60 seconds perform Disk Free Limit Notification	 
	When sensor state is Warning for at least 300 seconds perform Disk Free Limit Notification and repeat every 0 minutes	
	When condition clears after a notification was triggered perform Email to Admin	

Below the table, there are two sections for inheritance:

- Triggers that can be inherited from parent object(s)**: Two radio buttons are present. The first is 'Inherit all triggers from parent objects and use the triggers defined above' (unselected). The second is 'Only use the triggers defined above' (selected).
- Triggers that are defined in Library object(s)**: A table with columns for Type, Rule, and Inherited from, showing '(no triggers defined)' in the Type and Rule columns.

At the bottom of the screenshot, the text 'Setting a Notification Trigger for Disk Free Limit Notification' is displayed.

Step 6: Testing the Notification

Finally, test the notification that you created. You can immediately trigger this notification for test purposes:

- From the [main menu bar](#)²⁶³, select **Setup | Account Settings | Notification Templates**.
- For the respective notification template, click the **Edit** button and then **Send test notification**.

Then, check if the notification was triggered and delivered correctly, depending on the delivery method you defined before. If you do not get a notification (or a defined action is not executed) at all, check the notification logs: From the main menu bar, select **Logs | System Events | Notifications**. Look for the triggered notification in the table list (verifying that the notification delivery is set up correctly in general) and consider the corresponding message.

 See section [Logs](#)^[228] for more information.

More

This section provides information about additional options you have when working with notifications.

▪ Notification Settings:

You can create schedules to activate notifications only at specific times, for example, only on weekdays. In section **Notification Summarization** you can choose between various options to avoid message floodings. Furthermore, define which user groups will have access to edit this notification. For details about notification settings, refer to section [Account Settings—Notification Templates](#)^[331].

▪ Content of Emails:

You can individually adjust the subject, header, and footer of emails to your needs. See section [Account Settings—Notification Templates](#)^[331] for details about editing the subject. The article **How can I include my own logo into HTML emails?** in the Knowledge Base explains how to edit the header and footer of emails: <https://kb.paessler.com/en/topic/65782>

▪ Other Triggers:

An alternative to the state trigger would be to add a **Threshold Trigger**; then you would not need to set up limits explicitly, though, this trigger type would only be suitable for disk free sensors when using the trigger for single sensors, one by one. Free disk sensors have free space **in percent** as primary by default, other sensors have primary channels with the units bytes or seconds. However, threshold triggers only apply to the primary or total channel. General notification triggering by threshold might not work as expected for sensors of the "percentage" type. You can find all available triggers in section [Notifications](#)^[321].

▪ Add a Threshold Trigger to a sensor **directly**:

Go on a sensor's detail page and select the **Notification Triggers** tab. Click **Add Threshold Trigger**, select the desired channel, and provide the condition when this notification will be sent. In this example for free disk space, the setting would be "**When Free Bytes C: (%) channel is Below 20 for at least 60 seconds perform Disk Free Limit Notification**".

▪ Notifications with Libraries:

If your disk devices are spread over many groups, we recommend that you [use a PRTG library](#)^[325] for your disks. Choose **Libraries | All disk space sensors** from the main menu bar, go on the **Notification Triggers** tab, and add a state trigger as described above.

 Not all disk free sensor types might appear. You can add them to this library in the settings of the library node. There you can [filter by type or tag](#)^[325] and add missing sensors. You can also filter by priority and other sensor properties.

Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications
1 Setting up Notifications Based on Sensor Limits: Example

Edit Object Diskspace sensors ✕

Basic Library Node Settings

Library Node Name ⓘ
Diskspace sensors

Tags ⓘ
+

Node Display Settings

Linked Object ⓘ
Root » 🔍

Node Type ⓘ

Show a subtree of the device tree in the library
 Show a collection of filtered sensors in the library (max. 1000)

Filter By Type ⓘ

Show all sensor types
 Show specific sensor types only

Filter By Status ⓘ

Show all sensor states
 Show sensors with a specific status only

Filter By Tags ⓘ

Show all tags
 Show objects with specific tags only

Select Tags ⓘ

diskspacesensor ✕ smbdiskspacesensor ✕ + disk
diskfree
diskfreesensor
diskspacesensor
logicaldisk
physicaldisk
smbdiskspacesensor

Filter By Priority ⓘ

Cancel OK

Settings of a Library with Diskspace Sensors

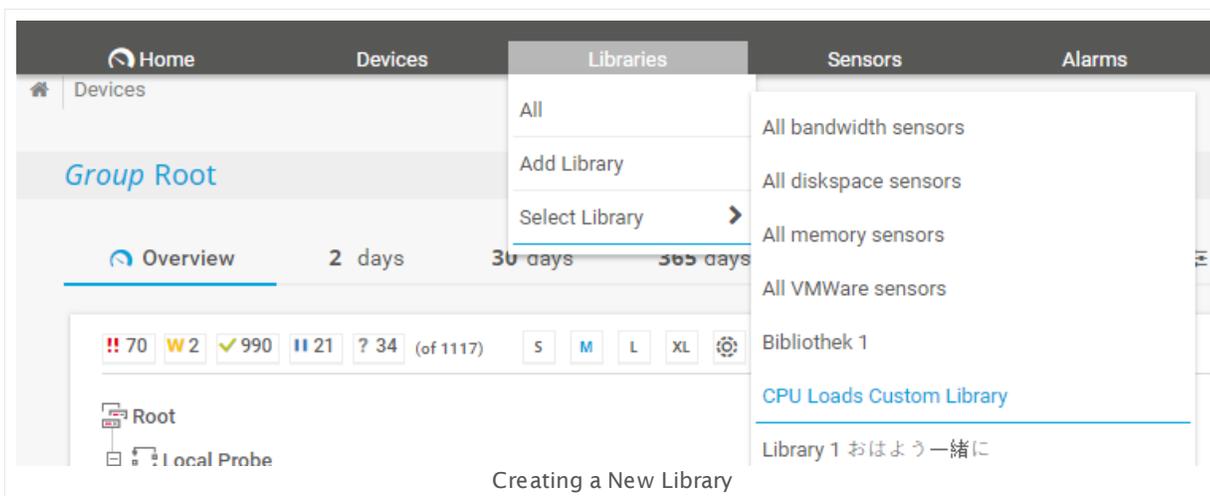
8.8.2 Setting up Notifications Based on Libraries: Example

What's so special about notifications set to whole libraries instead of single sensors? How do I set up libraries, and how do I get the most out of my library notifications?

This section describes how you can reorganize your devices or sensors by their function, and thereby create a new customizable view. This way you can monitor entire sections of your network with a single set of [notifications](#)³²¹⁶.

You can personalize these views and their notifications for your own use. Furthermore, you can grant and restrict permission to this view to other PRTG users or PRTG user groups, to give them direct access to some of the information in PRTG. By using libraries, you can make your notification management faster, easier, more powerful, and more refined.

Step 1: Setting up a New Library

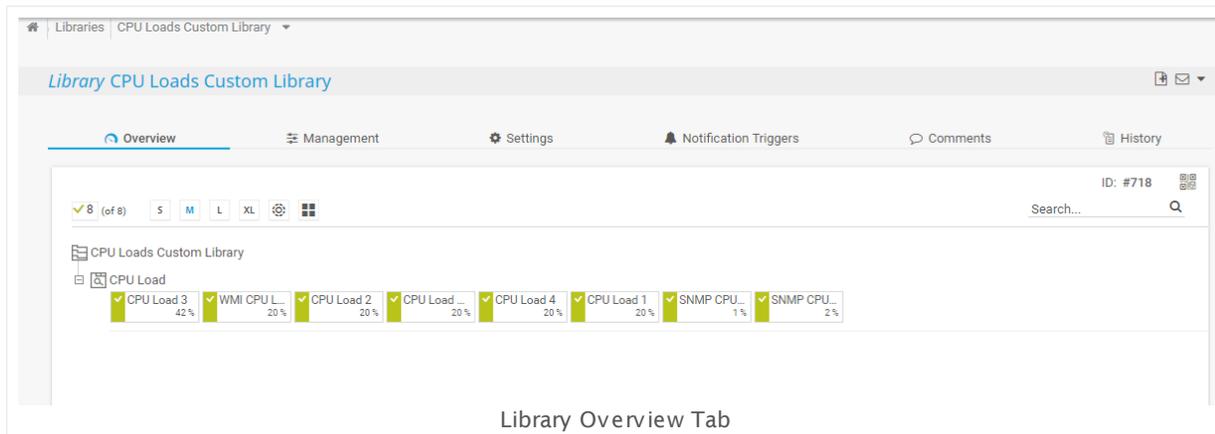


Create a new library:

- Hover over **Libraries** in the main menu bar and select **Add Library**.
- Give the library a meaningful name and assign it a [security context](#)³²⁴⁵. Possibly add some [Tags](#)¹³⁹¹ for easier organization.
- Optionally, assign access rights to your predefined user groups.
- Click **Create** to create the new library.
- The **Management** tab of the library opens.

Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications

2 Setting up Notifications Based on Libraries: Example



Add objects to your library:

- Click the **Add Library Node** button.
- The **Add Library** dialog opens.
- Define the **Node Display Settings**:
 - Choose a node from which the sensors will be taken (predefined: **Root**).
 - Select **Show a collection of filtered sensors in the library (max. 1000)** to filter (the subtree) further.

Choose from the following filter criteria:

- **Show specific sensor types only**: Add check marks to sensor types you want to include.
- **Show sensors with a specific sensor status only**: Choose from up, warning, down, or unusual.
- **Show objects with specific tags only**: Enter tags to include certain sensors.
- **Show objects with a specific priority only**: Priority "1" through "5" is possible.

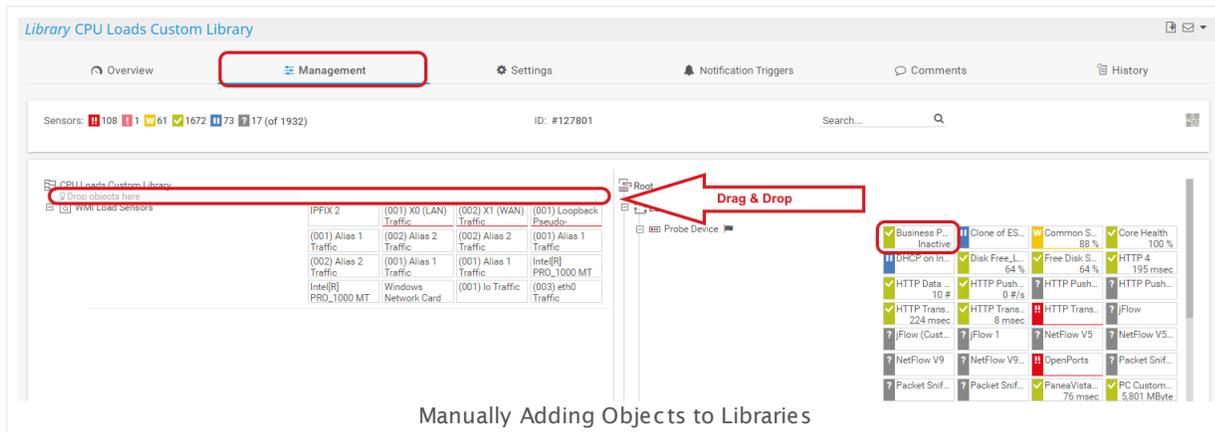
i The libraries are dynamic not static. When you add or remove sensors to your device tree that are of a type already specified here, the library will automatically update the displayed sensors. The same is true for the other three categories.

- Confirm via **OK**.
- The new library node appears.

i You can rearrange the nodes in any sequence you require. To manually add objects from the device tree, proceed as follows: Select the **Management** tab, click and hold an object from the right-hand device tree, then drag over to the **Drop objects here** area. This will transfer the entire content of the object to a new library node.

Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications

2 Setting up Notifications Based on Libraries: Example



Step 2: Specify Notification Triggers

You can use library notifications very much the same way as notifications for sensors or devices.

- In your library, click the **Notification Triggers** tab.
- Choose one of the various notification trigger types and configure it:
- **Add State Trigger** to send notifications about [sensor states](#) over a specified time period.
- **Add Speed Trigger** to send notifications when having too little or too much traffic over a specified time period.
- **Add Volume Trigger** to send notifications when a predefined amount of data in the specified interval is accumulated.
- **Add Threshold Trigger** to send notifications if a sensor channel value goes beyond or below a certain limit.
- **Add Change Trigger** to send change messages sent by your sensor (only certain sensors provoke change triggers).

Example: Library Notification

You monitor hundreds of servers and want to keep an eye on CPU utilization. Using the channel limits within the sensors would cause an overwhelming amount of alerts, because CPUs can easily spike to 100% load for one scanning interval, without necessarily indicating a problem.

Using libraries, it only takes you a couple of minutes to create a notification setup that will notify you when a CPU runs at more than 90% load for more than 5 minutes.

We recommend the following steps:

1. Create a custom library.
2. Add CPU sensors (via tag or type).
3. Add a threshold-based notification.

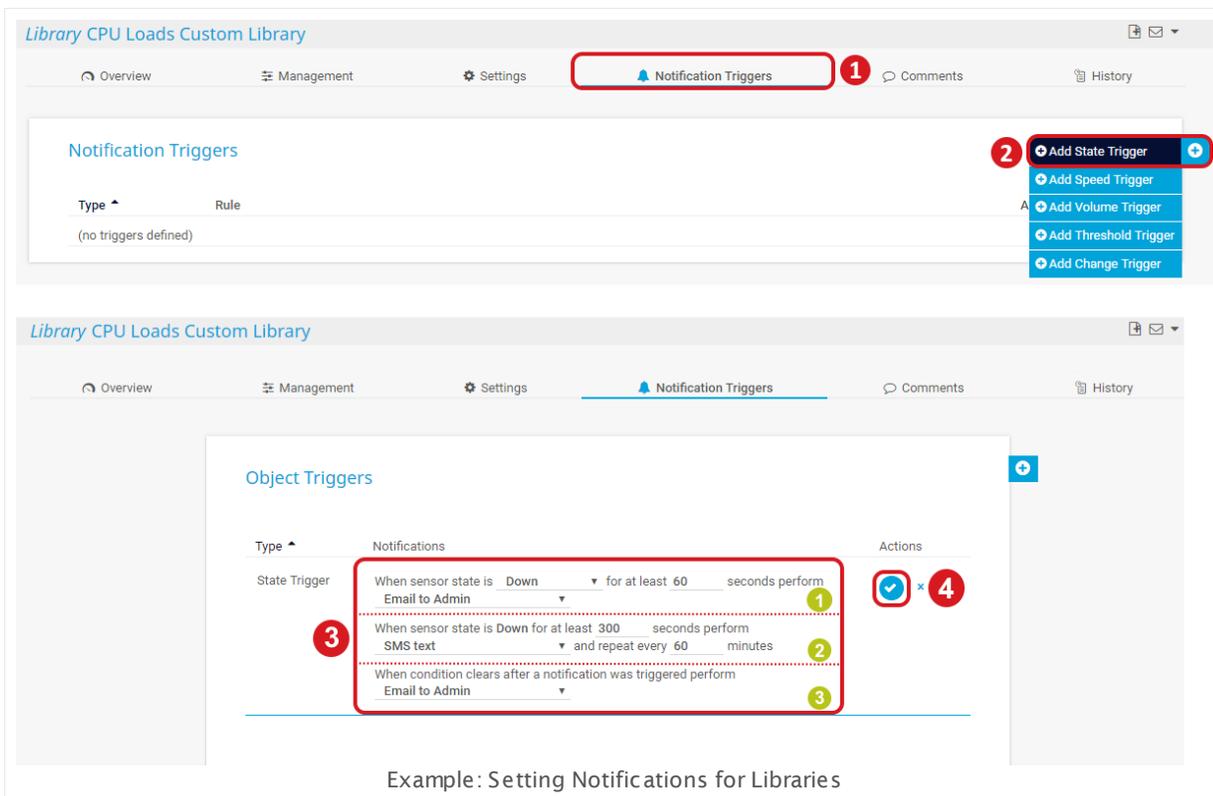
Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications

2 Setting up Notifications Based on Libraries: Example

4. Enjoy complete peace of mind!

Add a state trigger to your library:

- Select the **Notification Triggers** tab (1).
- Hover over  and select **Add State Trigger** (2) from the menu.
- Enter the desired notification specifications in the definition box (3), including:
 - initial parameters (triggering state, triggering state duration, notification type triggered), 
 - escalation parameters (triggering state is always the same, ongoing duration that triggers escalation, the type of the escalation notification triggered, and how often it is repeated), 
 - if the trigger parameters no longer apply, enter the type of notification to be triggered. 



The screenshot shows the PRTG Network Monitor interface. The top navigation bar includes 'Overview', 'Management', 'Settings', 'Notification Triggers' (highlighted with a red box and callout '1'), 'Comments', and 'History'. Below this, the 'Notification Triggers' section is shown with a table of triggers. A red box highlights the 'Add State Trigger' button (callout '2') and the 'Add State Trigger' button in the 'Object Triggers' configuration screen (callout '4'). The 'Object Triggers' configuration screen shows a table with three rows of triggers, each with a red box and a callout (3, 2, 3) indicating the configuration area.

Type	Notifications	Actions
State Trigger	When sensor state is Down for at least 60 seconds perform Email to Admin	 
	When sensor state is Down for at least 300 seconds perform SMS text and repeat every 60 minutes	
	When condition clears after a notification was triggered perform Email to Admin	

Example: Setting Notifications for Libraries

- An overview of all currently defined triggers appears.

On top of that, you may want PRTG to keep sending you **Tickets** when a lower load threshold is periodically exceeded. This low priority notification will remind you to keep an eye on a certain part of your network. Proceed likewise via the **Add Threshold Trigger** button.

 You are completely free to set multiple triggers of the same type, so you can define increasingly serious notifications, as well progressing through different notification actions (email, SMS text, etc.). For system-critical network components, we recommend that you always define two different notification triggers (for example, email and escalation SMS text message).

The next steps will be to review the notifications settings, summarization, and notification actions in the main menu under **Setup | Account Settings | Notification Templates**.

Step 3: Test, Troubleshooting, and Customization

To make sure the notification system works as desired, you can trigger test notifications out of PRTG.

- Click the **Edit** button next to a notification and select **Send test notification** under **Setup | Account Settings | Notification Templates**.
- Check if the test email and/or SMS text has arrived.

 In test notification messages, placeholders will not be resolved.

Troubleshooting: if you suspect a notification might not arrive, proceed as follows:

- Select **Setup | Account Settings | Notification Templates** from the main menu bar.
- Go to the notification action you have assigned in the library and click **Edit**.
- Review the notification setting so that:
 - The notifications are in the **Active** status.
 - The notifications have a [schedule](#)  that does not conflict with the library you just set up or currently pauses the notification.
 - The summarization method collects alarms for a certain period. Also consider the **Timespan for Summarizing Messages** value.
 - The user email addresses (phone numbers) specified for each user account are correct.
- Check the [Notification Delivery Settings](#)  under **Setup | System Administration | Notification Delivery**.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

- Review the [logs](#)  for system events of the type "Notification" and the respective notification's name.
- Repeat these steps for all your notifications.

 Sensors can perform simulated errors. Go to the library's **Overview** tab, right-click a sensor, and select **Simulate Error Status** from the context menu. You will see that the sensor status quickly changes and sends the following message: **Simulated error (code: PE034)**. This also triggers the notification.

 You can have the overall status of your library displayed as custom object on a map. See this Knowledge Base article: [How can I use a status icon of a device in Maps which only considers specific sensors?](#)

Part 8: Ajax Web Interface—Advanced Procedures | 8 Notifications
2 Setting up Notifications Based on Libraries: Example

More

Knowledge Base: How can I use a status icon of a device in Maps which only considers specific sensors?

- <https://kb.paessler.com/en/topic/59942>

8.9 Libraries

With the **Libraries** feature in PRTG you can create special views of your device tree with up-to-the-minute monitoring status information, arranged the way you want it.

Example of a Library

In this section:

- [Introduction](#) ³²³⁵
- [Start Libraries](#) ³²³⁶
- [Libraries List](#) ³²³⁷
- [Working with Libraries](#) ³²³⁷

See also this video tutorial: [PRTG Network Monitor – Libraries](#)

Introduction

Libraries are a powerful feature that enables you to create additional views of your device tree. These views are updated with the same scanning interval as your device tree, showing the same monitoring data, but arranged the way you want. This is useful if you want to display data in different ways, like depending on target groups or a specific use case.

For example, you can create a library that contains an overview of all your bandwidth monitoring sensors, regardless of the device they are running on.

The library features include:

- Create libraries containing nodes with monitoring objects from all over your configuration.

- Show data from different PRTG probes in one library.
- Show different branches of your device tree right next to each other.
- Arrange sensors in a tree-like view regardless of the device they are running on.
- Filter your entire tree (or parts of it) for sensor type, state, or tag, showing only matching sensors.

You can create libraries easily, using **drag&drop**.

PRTG comes with several pre-configured standard libraries, which you can use right away. You can also change or delete them, if you like. The following libraries are automatically created when you install PRTG for the first time (visible for the PRTG Administrator user). Some of them will initially be empty, but as you add more sensors, they will be filled automatically according to the filter settings defined for the nodes of the libraries:

- All bandwidth sensors
- All CPU load sensors
- All disk space sensors
- All memory sensors
- All VMware sensors
- Sensors grouped by priority
- Sensors grouped by state

 Sensors that are added to libraries are not counted against the maximum number of sensors of your license.

Start Libraries

Click **Libraries** in the [main menu](#)²⁶⁷ to view or add custom views of your network's status and monitoring data. Hover over **Libraries** to show menu items. Choose between:

LIBRARIES	
All	Open the Libraries overview list where you can view or add custom device tree views of your network status and monitoring data.
Add Library	Open an assistant to create ³²³⁸ a new library.
Select Library >	Open an existing library. Hover over Select Library to show more options. Follow the alphabetical menu path (it is specific to your setup) to view your libraries. Click a library to open it.

Libraries List

In the **All** view, you see a list of all existing libraries. Using the **Edit** buttons, you can perform the following actions.

- **Used by**: Show which other monitoring objects use this library.
- **Clone**: Create a [clone](#)³¹⁹³ of this library.
- **Delete**: Delete this library.
- **Settings**: Open this library and change the [settings](#)³²⁴⁵ of the library and its nodes.

Hover over  and select **Add Library** from the menu to add a new library.

Please also see [Working with Table Lists](#)²³⁷. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the [Multi-Edit Lists](#)³¹⁹⁷ section.

Working with Libraries

For detailed information on how to create and edit libraries, see the following sections.

- [Libraries Step By Step](#)³²³⁸
- [Management](#)³²⁴²
- [Libraries and Node Settings](#)³²⁴⁵
- [Context Menus](#)³²⁵¹

More

Video Tutorial: PRTG Network Monitor - Libraries

- <https://www.paessler.com/support/videos/prtg-basics/libraries>

8.9.1 Libraries Step By Step

In order to create a new library, follow the steps in this section. In the web interface, click on the **Libraries** entry in the main menu to show the libraries main screen.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

In this section:

- [Step 1: Add Library](#)  3238
- [Step 2: Add Library Nodes](#)  3238
- [Step 3: Set Library Node Display Settings](#)  3239
- [Step 4: View](#)  3240

Step 1: Add Library

- Hover over  and select **Add Library** from the menu to add a new library. An assistant is shown.
- Enter a **Library Node Name**.
- Define **Security Context**, **Tags** and **Access Rights** if you like.
- Click **Create**.

 For detailed information, see [Libraries Settings](#)  3245 section.

Step 2: Add Library Nodes

Click the **Management** tab. You will see a split screen:

- On the left side, your library is shown (empty in the beginning).
- On the right side, you see your device tree, as known from the device tree's [Management](#)  3229 tab.

Bandwidth Library in Management Mode

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new **Library Node**. Repeat this procedure as often as you wish until you have added all desired items to the library.

- ❗ When adding single sensors to the library, there can only be one sensor in one library node.
- ❗ Library nodes can contain up to 1,000 sensors.

You can also create nested library nodes by adding a new node underneath an existing one or to a group.

Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

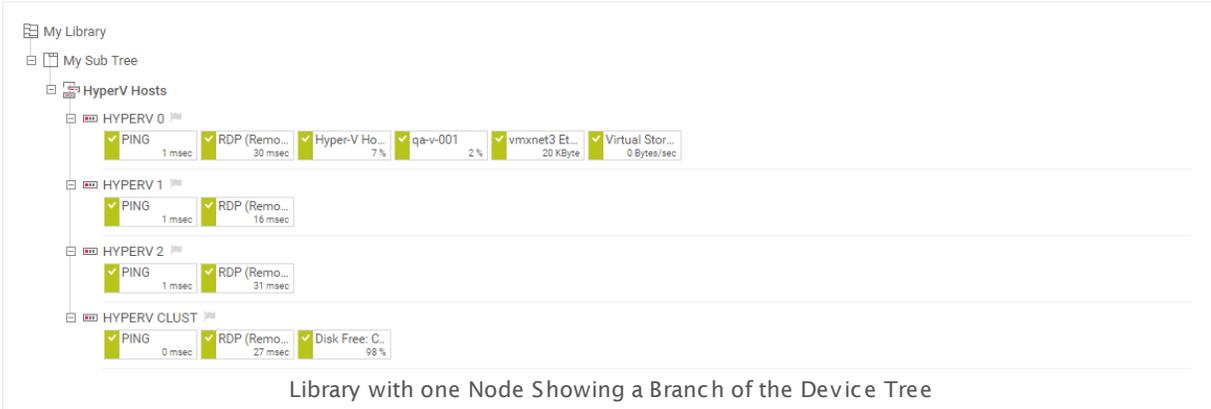
Step 3: Set Library Node Display Settings

You are still in the library **Management** tab.

Right-click the name of a **Library Node** and from the context menu, select **Edit | Settings...** to change the **Node Display Settings**. In this dialog, you can change the name of the library and its tags, as well as the linked object, node type, and filters.

These settings are available for each library node. You can choose to either show the **Linked Object** as a sub-tree of your device tree, or to view a collection of all sensors underneath the **Linked Object**.

When selecting the sub-tree view, the library node will just look like a branch in your device tree, as shown in the screenshot below for the library node named "My Sub Tree".



When selecting a sensor collection view, only the sensors underneath the **Linked Object** are shown, omitting probes, groups, and devices. You can additionally filter by certain sensor **Type**, **Status**, and **Tags**. Only matching sensors will be shown. The screenshot below shows the same **Linked Object** as above, but in sensor collection view, additionally filtered for sensors with a **bandwidthsensor** tag.



For detailed information, see [Libraries and Node Settings](#) (Overview—Library Node Display Settings) section.

Step 4: View

Click the **Overview** tab to see the final appearance of your library. You have the following options:

- Hover over an object to view a popup window with recent monitoring and status data.
- Use the sensor status selection bar to select which sensors you want to see for the library: Simply remove check marks for sensor states you want to hide.
 - ⓘ This function is the same you know from the device tree's [sensor status bar](#). The setting is reset the next time you open the library.

- Use the **Device Tree View** selection in the [page header bar](#)¹⁸⁵ to change the size of the library display.
 - ❗ This function is the same you know from the [device tree](#)¹⁸⁷.
- Use the **Search** box in the [page header bar](#)¹⁸⁵ to search the library for a string in object names. Matching objects will be shown full-colored, all others will be grayed out while the filter is active. Click the small x symbol in the search field to reset the filter.
 - ❗ This function is the same you know from the [device tree](#)¹⁸⁵.

It depends on the library's access rights and the currently logged in user account if it will be visible to other PRTG users. Also, clicking objects in the library (for example, sensors) will lead to more detailed information about the object or to an error message indicating insufficient access rights—depending on user account and access rights.

 In libraries, you can right-click objects to access the [Context Menus](#)³²⁵ of nodes and the library itself. You can also set up notifications to entire libraries, see our example chapter [here](#)³²⁹

More

Video Tutorial: Libraries in PRTG

- <https://www.paessler.com/support/videos/prtg-basics/libraries>

8.9.2 Management

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Click the **Management** tab. You will see a split screen:

- On the left side, your library is shown (empty in the beginning).
- On the right side, you see your device tree, as known from the device tree's [Management](#) tab.

The screenshot displays the PRTG Network Monitor Management interface. The top navigation bar includes tabs for Overview, Management (selected), Settings, Notification Triggers, Comments, and History. Below the navigation bar, there are statistics: 55 errors, 105 warnings, 1640 OK, and 20 critical (of 1820 total). The main area is split into two panels:

- Left Panel (Library):** Titled "Library All bandwidth sensors". It shows a list of sensors categorized by type (e.g., Local Area, Ethernet-WFP Native, Ethernet-Traffic). At the bottom, there are buttons for "Add Library Node" and "Add Group".
- Right Panel (Device Tree):** Titled "Root". It shows a hierarchical tree of devices and their associated sensors. The tree includes:
 - Local Probe: Core Health (100%), Probe Heal... (100%), System He... (100%), Common S... (100%), Disk Free (79%), Intel[R] 825... (445 kbit/s), and SNMP CPU...
 - Network Discovery: HTTP (151 msec)
 - Network Infrastructure: Gateway: gw (PING: 0 msec, HTTP: 93 msec)
 - DNS/DHCP/ADS: PING (1 msec), RDP (Rem...) (15 msec), DNS (4 msec), CPU Load (3%), Memory (83%), Disk Free (71%), Pagefile Us... (0%), Uptime (9 d 12 h), Gigabit-Net... (1,672 kbit/s), Disk IO_To... (<1%), Disk IO 0 C... (<1%), Volume IO ... (70%), and Volume IO ... (16%)
 - Exchange: PING (1 msec), SSL Certifi... (1,501), SSL Certifi... (1,501), SSL Securi... Weak Proto... (1,501), HTTPS (94 msec), RDP (Rem...) (15 msec), IMAP (11 msec), POP3, SMTP, and CPU Load

At the bottom of the screenshot, the text "Bandwidth Library in Management Mode" is displayed.

Add and Change Library Nodes

From the device tree on the right side, drag objects and drop them on the library on the left side. Each dropped object will be added immediately as a new **Library Node**. Repeat this procedure as often as you wish until you have added all desired items to the library.

i When adding single sensors to the library, there can only be one sensor in one library node.

i Library nodes can contain up to 1,000 sensors.

You can also create nested library nodes by adding a new node underneath an existing one or to a group.

Drag and drop nodes within the library to change their position. If you want to change the monitoring object that is associated with a library node, you can change the **Linked Object** in the node's settings.

Set Library Node Display Settings

Right-click the name of a **Library Node** and from the context menu, select **Edit | Settings...** to change the **Node Display Settings**. In this dialog, you can change the name of the library and its tags, as well as the linked object, node type, and filters.

These settings are available for each library node. You can choose to either show the **Linked Object** as a sub-tree of your device tree, or to view a collection of all sensors underneath the **Linked Object**.

When selecting the sub-tree view, the library node will just look like a branch in your device tree, as shown in the screenshot below for the library node named "My Sub Tree".

Library with one Node Showing a Branch of the Device Tree

When selecting a sensor collection view, only the sensors underneath the **Linked Object** are shown, omitting probes, groups, and devices. You can additionally filter by certain sensor **Type, Status, and Tags**. Only matching sensors will be shown. The screenshot below shows the same **Linked Object** as above, but in sensor collection view, additionally filtered for sensors with a **bandwidthsensor** tag.

Library with one Node Showing a Collection of Bandwidth Sensors Only

📘 For detailed information, see [Libraries and Node Settings](#) ³²⁴⁵ (Overview—Library Node Display Settings) section.

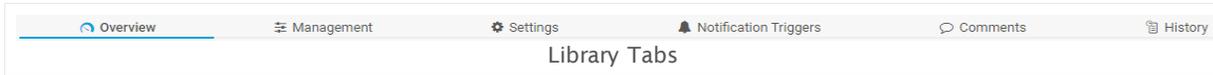
Context Menus

On right-click, there are different context menus available—in the **Management** as well as in the **Overview** tab.

 For detailed information, see [Context Menus](#)³²⁵¹ section.

8.9.3 Libraries and Node Settings

Using the libraries tabs you can access all functionalities and settings for a library.



Overview

Click the **Overview** tab any time to show the current state of your library.

Library Node Display Settings

While in the **Overview** tab, click the name of a **library node** to change its settings. Or, while in the **Management** tab, right-click a library node's name and select **Edit | Settings...** from the context menu. In both cases, the following settings are shown.

-  You can only change the settings of a node if it already contains monitoring objects like groups, devices, or sensors.

BASIC LIBRARY NODE SETTINGS

Library Node Name	Enter a meaningful name for the library node.
Security Context	<p>Define the security context for the Overview tab of the library. Choose a PRTG user account to define which objects will be visible. All users with access to the library will see the same content in this library as the security context user will see.</p> <p> Only sensors that are visible in the library will trigger a library notification.</p>
Tags	<p>Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the library. Tags are not case sensitive.</p> <p> It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).</p>

NODE DISPLAY SETTINGS

Linked Object	Click the reading-class symbol to change the object that is linked to this library node. The Object Selector ^[240] will appear.
Node Type	<p>Select what you want to view for this library node. Choose between:</p> <ul style="list-style-type: none">▪ Show a subtree of the device tree in the library: View all objects underneath the linked object as a device tree.▪ Show a collection of filtered sensors in the library (max. 1000): View all sensors underneath the linked object (only sensors are shown). You can combine several filters with each other (see below). <p> The node can show up to 1,000 sensors, surplus sensors are discarded.</p>
Filter By Type	<p>This option is only visible if collection of sensors is enabled above. Select if you want to filter the sensor list by a certain type. Choose between:</p> <ul style="list-style-type: none">▪ Show all sensor types: Do not filter for a sensor type.▪ Show specific sensor types only: Filter the sensor list of the linked object for certain sensor types. <p> This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.</p>
Select Sensor Types	<p>This option is only visible if filtering by type is enabled above. A list of all sensor types is shown, currently available sensor types are shown in bold letters for your convenience.</p> <p>Set a check mark in front of each sensor type you want to include in the library node view. You can also select and deselect all items by using the check box in the table head.</p> <p> This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.</p> <p> You cannot filter for sensor types that are defined in PRTG Mini Probes.</p>
Filter By Status	<p>This option is only visible if collection of sensors is enabled above. Choose between:</p> <ul style="list-style-type: none">▪ Show all sensor states: Do not filter for a sensor status.

NODE DISPLAY SETTINGS

	<ul style="list-style-type: none"> ▪ Show sensors with a specific status only: Filter the sensor list of the linked object for sensors in certain states.
Select Sensor States	<p>This option is only visible if filtering by sensor state is enabled above. A list of sensor states is shown. Set a check mark in front of each status you want to include in the library node view. Choose from:</p> <ul style="list-style-type: none"> ▪ Unknown ▪ Up ▪ Warning ▪ Down ▪ Paused ▪ Unusual ▪ Down (Acknowledged) ▪ Down (Partial) <p>You can also select and deselect all items by using the check box in the table head.</p> <p> This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.</p>
Filter By Tags	<p>This option is only visible if collection of sensors is enabled above. Choose between:</p> <ul style="list-style-type: none"> ▪ Show all sensor tags: Do not filter for a tag. ▪ Show objects with specific tags only: Filter the sensor list of the linked object for sensors with a certain tag¹³⁹. <p> The tag of a sensor can also be inherited¹³⁷ by a parent object.</p>
Select Tags	<p>This option is only visible if collection of sensors is enabled above. Enter one or more tags¹³⁹ of sensors that you want to include in the library node view. You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, +snmp;-wmi (must have the tag snmp and must not have the tag wmi).</p> <p> This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.</p>

NODE DISPLAY SETTINGS

Filter By Priority

This option is only visible if collection of sensors is enabled above. Choose between:

- **Show all priorities:** Do not filter for the [priority setting](#)³²⁴² of a sensor.
- **Show objects with specific priority only:** Filter the sensor list of the linked object for sensors with specific priority.

 The priority setting of a group, device, or sensor is ignored here; only the priority setting of the sensor itself is regarded.

Select Priority

This option is only visible if collection of sensors is enabled above. Define which priority setting sensors must have to appear in this collection. Set a check mark in front of each priority you want to include in the library node view. Choose from:

- ***** (highest)
- *****
- ****
- ***
- **
- * (lowest)

 This filter is applied in real-time. If the configuration underneath the linked object changes, the library node will show matching sensors accordingly.

Click **OK** to store your settings. If you close the dialog box via the **X**, all changes to the settings will be lost!

 After applying filters it might take several seconds for the changes to become visible. This is due to internal filter processes running in the background.

Management

Click the **Management** tab to edit the contents of your library, for example, to add items to the library using drag&drop.

 For more details, see section [Management](#)³²⁴².

Settings

Click the **Settings** tab to open a library's general settings.

BASIC LIBRARY SETTINGS

Library Name	Enter a meaningful name for the library.
Tags	Enter one or more tags ^[139] , separated by space or comma. For example, you can use tags later to search for the library. Tags entered here are inherited ^[137] to all library nodes underneath. Tags are not case sensitive.

ACCESS RIGHTS

Click  to disrupt the inheritance. See section [Inheritance of Settings](#)^[137] for more information.

User Group Access Define which user group(s) will have access to the object you're editing. A table with user groups and types of access rights is shown: It contains all user groups from your setup. For each user group, you can choose from the following access rights:

- **Inherited:** Use the access rights settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object neither shows up in lists nor in the device tree. Exception: If a child object is visible to the user, the object is visible in the device tree, though not accessible.
- **Read:** Users in this group can see the object and review its monitoring results.
- **Write:** Users in this group can see the object, review its monitoring results, and edit the object's settings. They cannot edit access rights settings.
- **Full:** Users in this group can see the object, review its monitoring results, edit the object's settings, and edit access rights settings.

You can create new user groups in the [System Administration—User Groups](#)^[338] settings. To automatically set all objects further down in the hierarchy to inherit this object's access rights, set a check mark for the **Revert children's access rights to inherited** option.

 For more details on access rights, see the section [User Access Rights](#)^[158].

 When giving access rights to a user group, all members of this user group will be able to see the objects in the library just as seen by the user who originally created the library.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notification Triggers

You can define notification triggers for any kind of object libraries. This is even possible for dynamic libraries, which can change with every scanning interval, for example, when you filter a library for the sensor status or priority.

 For details about how to use notifications, see section [Notifications](#) .

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Delete

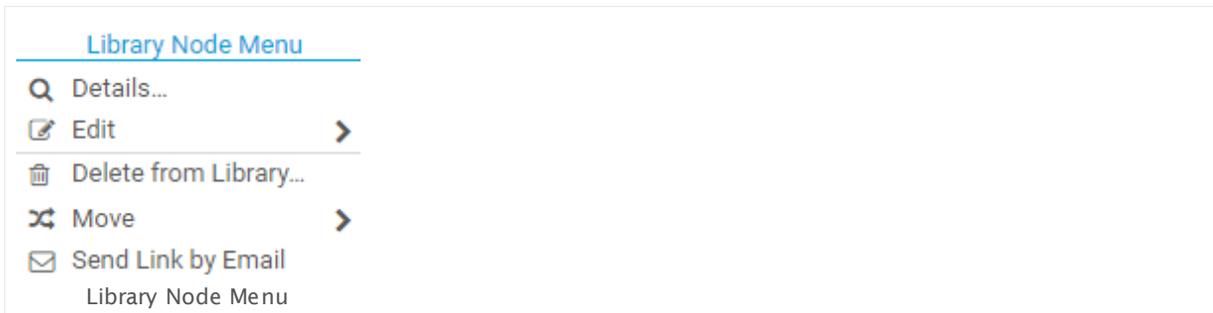
You can delete the entire library any time, simply right-click a library's name and select **Delete...** from the context menu.

8.9.4 Context Menus

On right-click, there are different context menus available.

Library Node Menu

While in the **Overview** tab or the **Management** tab of a library, right-click any library node to show its context menu.



- Select either **Details...** or **Edit | Settings...** to get to the [Libraries and Node Settings](#)³²⁴⁵.
 ⓘ While on the **Overview** tab, these settings are also accessible via left-click on the node's name.
- **Edit | Rename...** will give you an option to rename the library node quickly.
- **Delete from Library...** will remove this library node from the current library.
 ⓘ This will not delete any objects in your device tree.
- The **Move | ...** options will move the library node up and down within the library.
- Select **Send Link by Email** to open a new email using your system's standard email client. It will contain a direct link to the page you're currently viewing.

Monitoring Objects Menus

In libraries are the same [Context Menus](#)²⁴⁷ available you already know from the device tree. With one exception: While accessing these menus within libraries, the **Move** and **Delete** options are disabled to avoid accidental changes to your device tree.

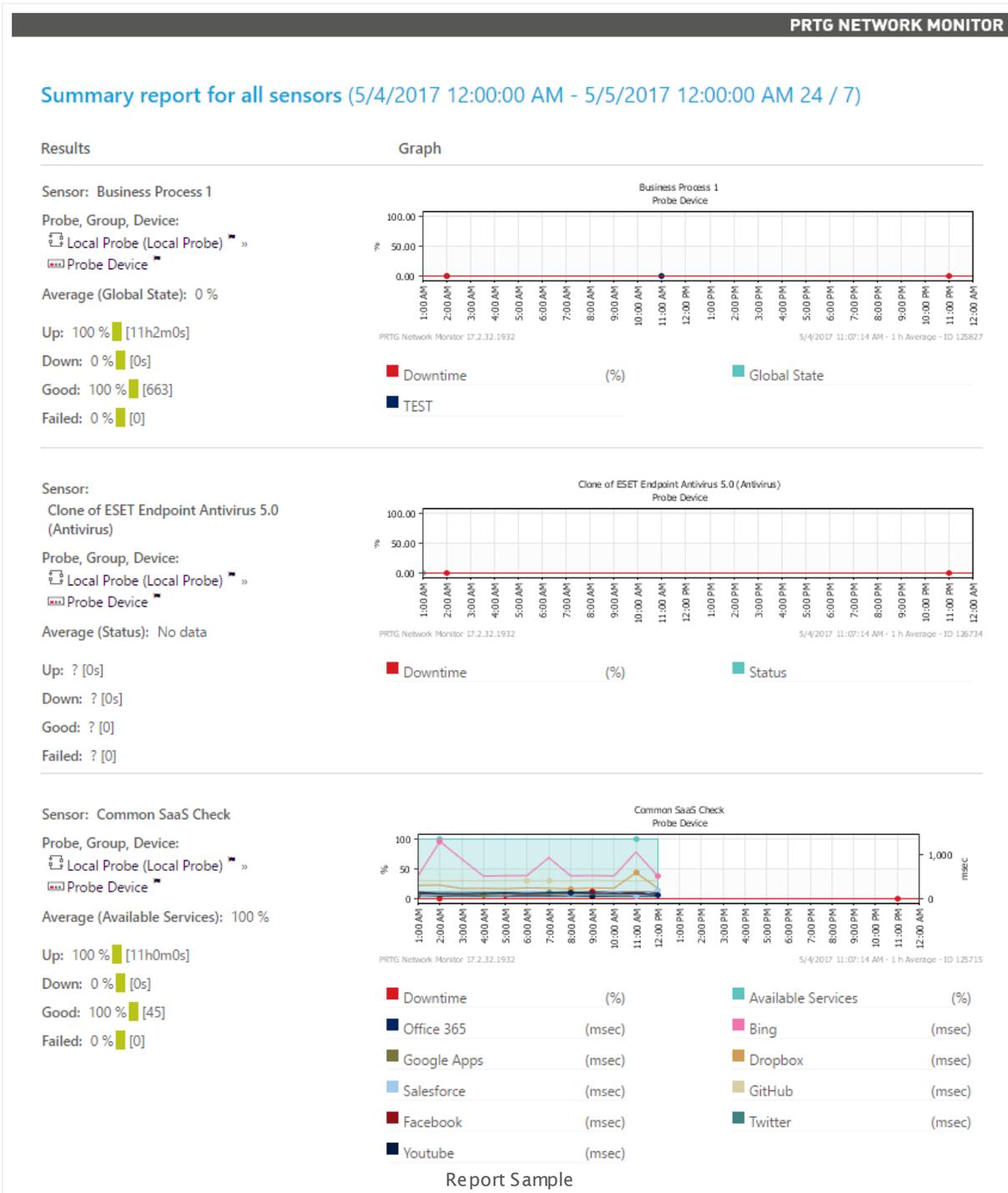
8.10 Reports

You can use reports to analyze historic monitoring results over a specified time such as one or more days, one month, or an entire year, and for your system configuration. You can create reports for all or only for certain sensors.

Introduction

PRTG includes a powerful reporting engine for the ad-hoc as well as scheduled report generation in HTML, PDF, CSV, and XML format. This means that you can run reports on demand or on a regular basis (for example, once a day or once a month). Furthermore, you can create reports for a single sensor or for a whole range of sensors. It is also possible to [create HTML reports of your system configuration](#)³²⁵².

The content and layout of the report is controlled by the report template of your choice and is the same for all sensors in a report. The report time that is shown in data tables and data graph legends depends on the system time of your PRTG core server, not on the [timezone settings](#)³³⁸⁰ of the current user account.



The sample report above shows the report data for devices on a local probe. You can see graphs for the preceding week, plus data tables with numeric results.

Start Reports

Click **Reports** in the [main menu](#)²⁷¹ to view or add reports of your monitoring data. Hover over **Reports** to show other menu items. Choose between:

REPORTS

- All Open the **Reports** overview page where you can view or add reports of your monitoring data.
- Add Report Open an assistant to directly [add](#)³²⁵⁷ a new report.
- Select Report > Open an existing report. Point to **Select Report** to show other menu items. Follow the menu path (it is specific to your setup) to select a report.
- Configuration Reports > Create reports for maps, reports, users & user groups, and system configuration to document changes to the configuration. Point to **Reports | Configuration Reports** to see the [available configuration reports](#)³²⁵⁶.

Reports Overview

Reports Show Filters ▾

Object ▾	Template ▾	Security Context ▾	Period ▾	Schedule ▾	Email ▾	Status ▾	Next Run ▾	Last Run ▾	# Sensors ▾	
<input checked="" type="checkbox"/> Active Directory	Graph 1 min interval, Table 1 ...	PRTG System Administrator	Month	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Diskfree Sensors	Graph 24h interval, Table 24h ...	PRTG System Administrator	Week	None		Idle	-	24.10.2017 11:20:46 (11 Sen...	11	
<input checked="" type="checkbox"/> Summary report for all sen...	List of sensors (with 1h graph)	PRTG System Administrator	Day	None		Idle	-	25.10.2017 09:02:53 (224 Se...	224	
<input checked="" type="checkbox"/> Top 100 Busy/Idle Process...	Data Table (5 min interval)	PRTG System Administrator	Day	None		Idle	-	18.01.2017 13:51:26 (4 Sens...	4	
<input checked="" type="checkbox"/> Top 100 Fastest/Slowest ...	Highest and lowest 5 minute ...	PRTG System Administrator	Day	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Top 100 Fastest/Slowest P...	Highest and lowest 5 minute ...	PRTG System Administrator	Day	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Top 100 Free/Full Disk Spa...	Highest and lowest 5 minute ...	PRTG System Administrator	Day	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Top 100 Most/Least Used ...	Highest and lowest 5 minute ...	PRTG System Administrator	Day	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Top 100 Most/Least Used ...	Highest and lowest 5 minute ...	PRTG System Administrator	Day	None		Idle	-	-	0	
<input checked="" type="checkbox"/> Top 100 Uptime/Downtime...	Top 100 Uptime/Downtime (b...	PRTG System Administrator	Day	None		Idle	-	-	0	

List of Reports

In the **All** view, you see a list of all existing reports for monitoring data. Every section shows information about one report:

- **Object**: Shows the name of the report.
- **Template**: Shows the name of the template that this report uses.
- **Security Context**: Shows the user account that PRTG uses to run the report.
- **Period**: Shows the time span that the report covers.

- **Schedule:** Shows if you set a schedule to regularly execute the report automatically.
- **Email:** If you set a schedule **and** an email address in the report settings, this shows the email address to which PRTG sends the report automatically.
- **Status:** Shows the current status of the report.
- **Next Run:** If you set a schedule in the report settings, this shows when PRTG runs the report the next time.
- **Last Run:** If you set a schedule in the report settings, this shows when PRTG ran the report the last time.
- **Number of Sensors in Last Run:** Shows about how many sensors the report includes data.

Please also see [Working with Table Lists](#)²³⁷. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the [Multi-Edit Lists](#)³¹⁹⁷ section.

Hover over  and select **Add Report** from the menu to add a new report, or click the name of an existing report to view and edit its settings. You can also run a pre-configured report easily by clicking its name and then using the options in the **Run Now** tab.

 For both options, see the [Reports Step By Step](#)³²⁵⁷ section.

 You can only [run configuration reports](#)³²⁵⁴ via the main menu.

Working With Reports

For detailed information on how to create, edit, and schedule reports, see the following sections:

- [Reports Step By Step](#)³²⁵⁷
- [View and Run Reports](#)³²⁶¹
- [Report Settings](#)³²⁶⁵

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when calculating data for large time spans. Data is then averaged regardless of the selected average interval.

TIME SPAN IN REPORT	MINIMUM LEVEL OF DETAIL (AVERAGE INTERVAL)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or larger

Reports for time spans of more than 500 days are not possible. If you enter a longer time span, it will automatically be shortened to 365 days.

 Under certain circumstances, the resulting report may contain a time span that differs to the defined start and end date because of internal averaging processes. When averages are greater than 1 hour and they do not equal 24 hours and they are combined with certain time spans, it might happen that resulting datapoints are asynchronous to the time spans. Please especially consider this behavior when you use [API](#)³⁶⁰⁶ calls to generate reports.

Configuration Reports

Configuration reports are a special type of reports and show the current PRTG configuration. They are available for **Maps**, **Reports**, **Users & User Groups**, and **System Configuration**. PRTG generates configuration reports and displays them in a new browser window as an HTML page in the common PRTG report style (like, for example, [Historic Data Reports](#)²⁰⁴ of sensors). You can use configuration reports, for example, to file and document changes to the configuration of your PRTG installation.

Configuration reports contain the same information as you can see on the overview pages of [Maps](#)³²⁷⁸, [Reports](#)³²⁵², as well as on the system administration tabs [User Accounts](#)³³⁷⁶ and [User Groups](#)³³⁸³. The configuration report **System Configuration** includes the current system administration settings of the tabs [User Interface](#)³³⁴³, [Monitoring](#)³³⁵⁵, [Notification Delivery](#)³³⁶¹, [Core & Probes](#)³³⁶⁸, and [Cluster](#)³³⁹⁴.

 Configuration reports are interactive so you can click available links to go to the corresponding webpage in the PRTG web interface.

Related Topics

- [Review Monitoring Data](#)¹⁹⁸
- [Historic Data Reports](#)²⁰⁴

8.10.1 Reports Step By Step

To create a new report or to run an existing one, follow the steps in this section. In the PRTG web interface, click the **Reports** entry in the main menu to show the reports main screen.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Quick Start: Run an Existing Report

PRTG is delivered with several pre-configured reports. To use one of them, click a report's name in the reports main screen and select the **Settings** tab. The next steps are the same as for completely new reports. Although some settings are already given, we recommend that you check them. For example, check the sensors that are included in the report. For some reports that come with PRTG, there are no sensors added yet. Continue with [Step 3: Define Additional Options](#)³²⁵⁹ in this section.

Step 1: Add Report

Hover over  and select **Add Report** from the menu to add a new report. An assistant appears where you can define various settings. First, enter a meaningful **Report Name**.

Add Report

Basic Report Settings

Report Name ⓘ

Report

Tags ⓘ

Template ⓘ

<please select a file> ▼

This field is required.

Security Context ⓘ

PRTG System Administrator ▼

Timezone ⓘ

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▼

Paper Size ⓘ

None
 A4
 A3
 A2
 Legal
 Letter
 Ledger

Orientation ⓘ

Portrait
 Landscape

Add Report Assistant

Step 2: Select a Template

In the **Template** option, select one of the report templates from the list. This defines the overall look of your report and how detailed (regarding the intervals) monitoring data is included. If you are not sure yet, try a template that appears most suitable to you. You can still change all settings later.

 For a detailed description of the available template options, see section [Report Settings](#) .

Step 3: Define Additional Options

Select a **Security Context** (best choose **PRTG System Administrator**, if available), your **Timezone**, and the **Paper Size** for PDF generation.

 For detailed information, see section [Report Settings](#) .

Step 4: Select Nodes and Sensors

Choose the sensors you want to include in the report. When running a [cluster](#) , define the **Cluster Node** the monitoring data is taken from first. Select a specific node from the list. If you select **All nodes**, PRTG creates a report with data from all of your cluster nodes, but only the primary channel of every sensor appears in the report.

Every report shows monitoring results based on sensor data. There are two ways to include sensors in a report: You can either add sensors manually or by tag. In the **Include Sensors by Tag** field, enter one or more tags that match the sensor range you want a report for.

For example, enter the tag **bandwidthsensor** to include all sensors that measure bandwidth (or select it from the list of tags that PRTG suggests). PRTG provides this tag by default when you add any bandwidth sensor, so the tag typically gathers all bandwidth sensors, unless you configured your system differently. You can enter several tags. Hit the enter key, or insert a comma or space after each tag and enter the next one. Use the **Filter Included Sensors by Tag** field to explicitly filter sensors with certain tags from the bulk of tags or manually selected sensors defined above.

Tagging is a great option to group sensors or other objects. For more information, see the [Tags](#)  section. You can also leave the tag fields empty and only choose specific sensors manually later.

Step 5: Decide on a Schedule and Additional Settings

In the **Report Schedule** section, choose if you want to run the report on a regular basis or on demand only. Also define which time **Period** will be covered by the report, if you want to show percentiles, if you want to generate CSV and XML data files for reports with data tables, and add report comments or special access rights.

 For detailed information, see the [Report Settings](#)  section.

 Scheduled reports are not executed on [failover nodes](#)³⁷²⁰ by default.

Save your settings. If you leave the current page, all changes to the settings will be lost!

Step 6: Check and Adjust the Sensors Included

After saving the settings, switch to the **Sensors Selected by Tag** tab to see a list of all sensors that you added with the tag(s) you defined in step 4. To change tags, go back to the **Settings** tab. You can additionally add sensors manually. To do so, switch to the **Select Sensors Manually** tab. The final report shows sensors from both manual and by tag selection.

 See section [Report Settings](#)³²⁷⁵ for detailed information and mind the [Remarks for Reports](#)³²⁶³.

Step 7: Run Report

Switch to the **Run Now** tab, select a period, and in the **Processing Options** select **View Report as HTML**. Click the **Run Report** button. PRTG generates the report in a new browser window or tab immediately. Depending on the number of selected sensors and the used template, it may take a few minutes until you see the report. If you do not want to wait, close the newly opened browser window or tab and select a PDF option in the **Processing Options**. Click the **Run Report** button again. The report is then generated in the background and you get a **ToDo ticket** or email once it is finished.

 For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: [Can I change the number of PDFs created by a report?](#)

More

Knowledge Base: Can I change the number of PDFs created by a report?

- <https://kb.paessler.com/en/topic/11863>

8.10.2 View and Run Reports

In the PRTG web interface, click **Reports** in the main menu bar to show the reports main screen. Click a report's name to select it. Use the various report tabs to access all functionalities and settings for the selected report.



Click **Go to all reports** at the bottom of the page to return to the list of all **Reports**.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Run Now

On the **Run Now** tab you can execute a report immediately with the settings configured. Please mind the [Remarks for Reports](#).

RUN REPORT "[Name]"

Report for

Define the time span covered by the report. Choose between:

- **Current Period:** Use monitoring data of the current period. The actual time span depends on the report period type defined in the report's [settings](#). It can be today, this week, this month, or this year.
- **Previous Period:** Use monitoring data of the last period. The actual time span depends on the report period type defined in the report's [settings](#). It can be yesterday, last week, last month, or last year.
- **Select a Period:** Use monitoring data of a period other than current or previous. Select below.
- **Select Date Range Manually:** Define a custom time span for the monitoring data that will be used. Set start and end date below.

Date Range

This selection is only visible if you enable the period option above. From the list, select a data range for which PRTG will generate the report. The shown time spans depend on the available monitoring data and on the report period type defined in the report's [settings](#). It can be days, weeks, months, or years.

RUN REPORT "[Name]"

Start Date	This selection is only visible if you enable the date range option above. Define the begin of the time span for which PRTG will generate the report. Use the date time picker to enter the date and time. Make sure you define a valid period.
End Date	This selection is only visible if you enable the date range option above. Define the end of the time span for which PRTG will generate the report. Use the date time picker to enter the date and time. Make sure you define a valid period.
Quick Range	This selection is only visible if you enable the date range option above. Choose between different pre-defined ranges by simply clicking the desired range. Each click changes the Start and End Date fields above accordingly.

PROCESSING OPTIONS

File Format and Delivery	<p>Define how you want to view the report. Choose between:</p> <ul style="list-style-type: none">▪ View Report as HTML: Directly view the report in your web browser. PRTG loads it in a new browser window or tab.▪ Create and store PDF and data files (available for templates with data tables): Create a PDF file and, depending on the Data Files settings ^[3265] of the report, CSV and XML files of the report and store them. Once finished, you will find it in the Stored Reports tab and a To Do ticket ^[230] will be created. By default, PRTG sends out a notification email to the administrator in this case.▪ Create PDF and data files (available for templates with data tables), store them, and send by email: Create a PDF file and CSV and XML files of the report, store the files, and send them via email once finished. <p> CSV and XML data files are only generated for report templates that include data tables.</p> <p> To create PDF files, ensure the print spooler service is running on the system with your PRTG server.</p> <p> Certain special characters, for example, 4-byte unicode characters, may not be displayed correctly in PDF reports. As workaround, generate an HTML report and save it as PDF.</p>
--------------------------	--

PROCESSING OPTIONS

 When generating reports with Internet Explorer 11, we recommend that you use one of the PDF options for optimal results.

 For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: [Can I change the number of PDFs created by a report?](#)

Target Email Address This setting is only available if you define above to send the report by email. Enter a valid email address to which PRTG will send the report.

 You can change the configuration for outgoing emails in the [System Administration—Notification Delivery](#) 3361 settings.

Compression This setting is only available if you define above to send the report by email. Define if you want to compress the attached report files before sending. Choose between:

- **Send files uncompressed:** PRTG will not compress the report files before they are sent by email but send the files in their original size.
- **Send all in one ZIP file:** PRTG will compress the report files to a ZIP file before they are sent by email.

Click the **Run Report** button to start report generation. Depending on the number of selected sensors, this may take a while. If you experience a long waiting time when generating HTML reports for immediate view, please consider using one of the PDF options. You can then view the report as soon as it has finished.

Remarks for Reports

- Any sensor graph in your report will only show channels that are enabled via the **Show in Graphs** option in the [Sensor Channels Settings](#) 3160.
- Reports show statistics for uptime (**Up** and **Down** in percent) and requests (**Good** and **Failed** in percent). Values between **5%** and **95%**, as well as **100%** and **0%**, are rounded to whole numbers without decimal places. Other values are shown with 3 decimal places.
- Due to rounding, the statistics in section **Sensor Status History** of the report might differ in a few seconds from the values in section **Uptime Stats**.
- Data reporting is limited to 5 requests per minute.
- Reports cannot show uptime or downtime data for the [Sensor Factory Sensor](#) 1720.

Part 8: Ajax Web Interface—Advanced Procedures | 10 Reports
2 View and Run Reports

- Create reports that include an appropriate amount of data. Reports may not work as expected if too many sensors with short scanning intervals have to be processed. Adjust your report size and time span that the report covers if necessary.

Stored Reports

In the **Stored Reports** tab you can view all PDF reports and data files created in the past. Click a name to open the report. Reports are stored until they are deleted according to the data purging settings of your PRTG configuration. You can set data purging limits for reports in the [System Administration—Core & Probes](#) settings.

Other Tabs

For all other tabs, see the [Report Settings](#) section.

More

Knowledge Base: Can I change the number of PDFs created by a report?

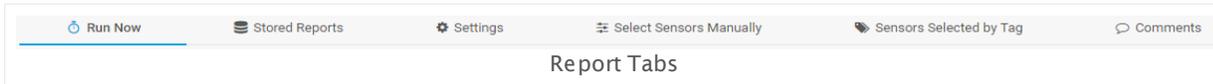
- <https://kb.paessler.com/en/topic/11863>

Knowledge Base: Why is there missing data in historical data reports?

- <https://kb.paessler.com/en/topic/61382>

8.10.3 Report Settings

In the PRTG web interface, click **Reports** in the main menu bar to show the reports main screen. Click a report's name to select it. Use the various report tabs to access all functionalities and settings for the selected report.



Click **Go to all reports** at the bottom of the page to return to the list of all **Reports**.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Run Now

On the **Run Now** tab you can execute a report immediately with the settings that you configured before.

 See section [View and Run Reports](#) ³²⁶¹ for details.

Stored Reports

On the **Stored Reports** tab you can view reports created in the past.

 See section [View and Run Reports](#) ³²⁶¹ for details.

Settings

Click the **Settings** tab to open the settings of a report. Please mind the [Remarks for Reports](#) ³²⁶³.

BASIC REPORT SETTINGS

Report Name	Enter a meaningful name to identify this report. The name of the report is used in reports lists ²⁷² and as headline of generated reports.
Tags	Enter one or more tags, separated by space or comma. For example, you can use tags later to search for the report. Tags are not case sensitive.

BASIC REPORT SETTINGS

 It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with round parentheses (()) or angle brackets (<>).

Template

Select a template for the report. The template defines the overall look of your report and in which detail (interval) the report shows monitoring data. PRTG includes several report templates out of the box. You can choose from templates in the following categories:

- **Data Table Only:** Create a report with data tables only. Choose from several intervals. Reports with this template also generate data files (CSV and XML) if set in the **Data Files** section of the report.
- **Graph Only:** Create a report with graphs only. Choose from several intervals. Reports with this template cannot generate data files (neither CSV nor XML).
- **Graph with Data Table:** Create a report with graphs and data table. Choose from several intervals. Reports with this template also generate data files (CSV and XML) if set in the **Data Files** section of the report.
- **List of Sensors:** Create a report in a compact sensor list style. This is available with and without graphs. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 100 Highest and Lowest:** Create a report with up to 100 objects with the highest and lowest average values. Choose from different intervals. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 10 Uptime/Downtime:** Create a report with up to 10 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Reports with this template cannot generate data files (neither CSV nor XML)
- **Top 100 Uptime/Downtime:** Create a report with up to 100 objects with the highest uptime and downtime each. You can choose between data in percent and hours. Reports with this template cannot generate data files (neither CSV nor XML)

 Monitoring data within an interval is averaged. See also the comment on data averaging in the [Reports](#) (Automatic Averaging) section.

 For information on how to modify templates, see this Knowledge Base article: [How do I modify PRTG's report templates?](#)

BASIC REPORT SETTINGS

Security Context	<p>Define the user account^[3376] that you want to use for access to your monitoring data. The report only contains objects that the selected user^[158] is allowed to view.</p> <p>Choose a PRTG user from the list. The available users depend on your configuration. By default, this is the user that created the report. PRTG System Administrator users can change this setting.</p>
Timezone	<p>Define the time zone to use for all date-specific settings in this report (see below^[3271]). Choose a time zone from the list.</p>
Paper Size	<p>Define the paper size in which PDF reports are created. Choose between:</p> <ul style="list-style-type: none">▪ None: Do not specify a paper format. The size is set automatically.▪ A4: Use German DIN A4 format.▪ A3: Use DIN A3 format.▪ A2: Use DIN A2 format.▪ Legal: Use North American legal paper format.▪ Letter: Use North American letter paper format.▪ Ledger: Use North American ledger paper format.
Orientation	<p>Define the page orientation for the data in PDF reports. Choose between:</p> <ul style="list-style-type: none">▪ Portrait: Use portrait mode for the page orientation.▪ Landscape: Use landscape mode for the page orientation. The landscape format is designed to properly show data tables of sensors with many channels. Other parts of the report will remain in portrait mode and do not re-size to the landscape format.

SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

Cluster Node	<p>This field is only visible when you run PRTG in Clustering^[130] mode. Define the cluster node from which the report will take monitoring data. Choose a cluster node from the list. The available options are specific to your configuration.</p>
--------------	---

SENSORS ("WHAT SENSORS WILL BE INCLUDED IN THE REPORT?")

By default, the current master node is set. Select **All nodes** to create a report with data from all of your cluster nodes.

- ❗ A report for all nodes includes data of the primary sensor channels only, not for other sensor channels. Be careful with big reports for all nodes because the report generation may slow down significantly.
- ❗ If you select a failover node, report and data files will not show data from the local probe or from a remote probe and might be empty or show "0" values.
- ❗ You can generate CSV and XML data files only for a single failover node. If you choose the option **All nodes**, the report will not create data files!

Add Sensors Manually If you want to manually choose the sensors included in this report, please save settings and switch to the [Select Sensors Manually](#) ³²⁷⁵ tab.

Include Sensors by Tag Define the sensors included in this report by [tag](#) ¹³⁹¹. Enter one or more tags. The report covers all sensors that have at least one of the tags. Please enter a string or leave the field empty.

You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, **+snmp;-wmi** (must have the tag **snmp** and must not have the tag **wmi**). See the section [Tags](#) ¹³⁹¹ for details.

❗ [Tags are inherited](#) ¹³⁹¹ automatically. So, for example, if you enter the tag of a [group](#) ¹³⁴¹ here, the report will include all sensors within this group. For detailed information, see the [Inheritance of Settings](#) ¹³⁷¹ section. For sensors you add by tag, the report includes all sensor channels automatically, except if you run a PRTG [cluster](#) ¹³⁰¹ and select **All nodes** in the **Cluster Node** selection above.

Filter Included Sensors by Tag Filter the included sensors further. This option works best in combination with manually added groups and devices. From the sensors that are implicitly added because of their parent objects, the report includes only the ones with the tags you enter here.

Enter one or more tags to include sensors in the report. Confirm a tag with enter, space, or comma key. Please enter a string or leave the field empty.

You can also use plus (must have) and minus (must not have) signs to categorize tags, for example, **+snmp;-wmi** (must have the tag **snmp** and must not have the tag **wmi**). See the section [Tags](#) ¹³⁹¹ for details.

SCHEDULE

Report Schedule	<p>Define at which time you want to run the report. Choose between:</p> <ul style="list-style-type: none">▪ No schedule (run interactive/on-demand only): Only use the options on the Run Now tab to start generating this report manually.▪ Every full hour: Run this report every 60 minutes.▪ Every day at a specific hour: Run this report every 24 hours.▪ Every specific day of a week: Run this report every 7 days. Specify the day below.▪ Every specific day of a month: Run this report on a specific day every month. Specify below.▪ The day after a quarter is finished (i.e. at 1. April for the 1. January - 31. March Quarter): Run this report for every quarter of the year.▪ Every specific date: Run this report on a specific date every year. Specify below.
Specify Hour	<p>This setting is only visible if you select a specific hour above. From the list, select the hour you want to run the report at. PRTG automatically chooses a suitable time within this hour, usually at the beginning of it.</p>
Specify Day	<p>This setting is only visible if you select the day of week or day of month option above. From the list, select a day of week or a date of the month you want to run the report.</p> <p>If you select Last, the report will always run on the last day of the month, regardless of how many days the month has. If you select a date that does not exist in every month, for example, February 31st, PRTG will automatically run the report on the last day of this month.</p>
Specify Date	<p>This setting is only visible if you select the specific date option above. Enter a valid date in the format DD.MM., for example, 31.12. The report runs annually on this date.</p>
Scheduled Processing	<p>This setting is only visible if you select one of the schedule options above. Define what to do with a finished report. Choose between:</p>

SCHEDULE

- **Save report to disk and send it by email:** Create a PDF file and, depending on the [Data Files](#) ³²⁷³ setting, data files of the report, store it, and send it via email. You find the report in your emails and on the **Stored Reports** tab. Define an email address below.
- **Save report to disk only:** Create a PDF file and, depending on the [Data Files](#) ³²⁷³ setting, data files of the report and store it. Once finished, you find them on the **Stored Reports** tab. You receive also a [ToDo ticket](#) ²³⁰¹ from PRTG. By default, PRTG sends out a notification email to the administrator in this case.
- **Send report by email only:** Create a PDF file and, depending on the [Data Files](#) ³²⁷³ setting, data files of the report and send them via email once finished. With this option the report is not permanently stored in PRTG. Define an email address below.

 For large PDF reports, PRTG automatically splits the output into separate files to avoid huge PDF files. You can change the number of sensors that PRTG includes into each PDF file by editing the report templates manually. For details, see this Knowledge Base article: [Can I change the number of PDFs created by a report?](#)

 Certain special characters, for example, 4-byte unicode characters, may not be displayed correctly in PDF reports. As workaround, generate an HTML report and save it as PDF.

Email Address

This setting is only visible if you select a send by email option above. Enter a valid email address to which PRTG sends the report. To enter more addresses, separate them by comma. PRTG sends a message with all recipients in the "To" field of the email.

 You can change the configuration for outgoing emails in the [System Administration—Notification Delivery](#) ³³⁶¹ settings.

Send to User Group

This setting is only visible if you select a send by email option above. From the list, choose a user group to send an email with the report to all members of this group. You can edit user groups in [System Administration—User Groups](#) ³³⁶³.

 If you define individual email addresses (see field above) and a user group, PRTG will send the report to the individual email addresses as well as to the members of the selected user group. In both cases, PRTG will send one message with all recipients in the "To" field of the email.

Compression

This setting is only visible if you select a send by email option above. Define if PRTG will compress the attached report files before sending them out. Choose between:

SCHEDULE

- **Send files uncompressed (default):** PRTG sends the report files by email in their original size.
- **Send all in one ZIP file:** PRTG will compress the report files to a ZIP file before they are sent by email.

PERIOD

Reported Period	Define the time span the report covers. Choose between: <ul style="list-style-type: none">▪ Current: Use monitoring data of the current period. Define the period type below.▪ Previous: Use monitoring data of the last period. Define the period type below.
Report Period Type	Define the type of period you want to create a report for. Choose between: <ul style="list-style-type: none">▪ Day▪ Week▪ Month▪ Quarter (January-March, April-June, etc.)▪ Year Depending on your selection, different period selections are shown below.
Day Period	This setting is only visible if you select day period type above. Define the hours when a day starts and ends. Choose from the list of hours. Default setting is 0:00-23:59 .
Week Period	This setting is only visible if you select week period type above. Define when the week starts and ends. Choose between: <ul style="list-style-type: none">▪ Monday-Sunday: A reported week starts on Monday.▪ Saturday-Friday: A reported week starts on Saturday.▪ Sunday-Saturday: A reported week starts on Sunday.
Month Period	This setting is only visible if you select month period type above. Define when the month starts and ends. Choose between:

PERIOD

- **1.-last day:** A reported month starts on the first and ends on last of the month.
- **15.-14.:** A reported month starts on 15th and ends on 14th of the month.

Year Period

This setting is only visible if you select year period type above. Define when the year starts and ends. Choose between:

- **1/1-12/31:** A reported year starts on January 1st.
- **7/1-6/30:** A reported year starts on July 1st.

Report only for specific hours-of-day (Schedule)

Include certain time spans within the defined period only. If a schedule is selected, the report will include only monitoring data for specified hours or weekdays within the defined period. Select **None** to include all available monitoring data in the report, or choose a schedule.

For example, select the schedule **Weekdays** to exclude all weekends from the report. The available schedules depend on your configuration.

 For more information, see the [Account Settings—Schedules](#) section.

INCLUDE PERCENTILES

Percentile Results

Define if you want to include an additional [percentile calculation](#)  of your data in the report. Choose between:

- **Do not show percentiles:** PRTG does not use a percentile formula to calculate your monitoring results. It will show only the standard values.
- **Show percentiles:** PRTG adds a column to the result data tables that shows percentiles for every sensor channel.

 Percentiles are not available for all report templates. If a template does not support percentiles, they will simply not show up in the report, even when you enable this setting.

Likewise, percentiles are not available in a cluster setup if you choose the option **All Nodes** in the **Cluster Node** setting in the sensor section above.

INCLUDE PERCENTILES

Percentile Type	<p>This setting is only visible if you select Show percentiles above. Enter the percentile type you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter "95" here and 5 % of peak values will be discarded.</p> <p>Please enter an integer value.</p>
Percentile Average Interval	<p>This setting is only visible if you select Show percentiles above. Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is 300 seconds (5 minutes). This means that PRTG takes 5 minute averages as basic values for the percentile calculation. Please enter an integer value.</p>
Percentile Mode	<p>This setting is only visible if you select Show percentiles above. Choose the mode for percentile calculation:</p> <ul style="list-style-type: none">▪ Discrete: PRTG takes discrete values to calculate percentile results.▪ Continuous: PRTG interpolates between discrete values and bases the calculation on interpolated values.

DATA FILES

CSV / XML Files	<p>Define if you want to generate CSV and XML files for data tables in the report in addition to the PDF. Choose between:</p> <ul style="list-style-type: none">▪ Do not include data files: PRTG will not generate CSV or XML files for the report but only a PDF file.▪ Include CSV files only (available for templates with data tables): PRTG will generate and store CSV files in addition to the PDF. CSV data files are only generated if the report uses a template with data tables.▪ Include XML files only (available for templates with data tables): PRTG will generate and store XML files in addition to the PDF. XML data files are only generated if the report uses a template with data tables.▪ Include all data files (available for templates with data tables): PRTG will generate and store CSV and XML files in addition to the PDF. CSV and XML data files are only generated if the report uses a template with data tables.
-----------------	--

DATA FILES

 If you run PRTG in a cluster, the report will not generate data files if you select **All nodes** in the [sensors selection](#)³²⁶⁷ above. Please specify a single failover node to get data files.

REPORT COMMENTS

- Introductory Comment** Enter your custom text that will show up on top of the first page of your report. Please enter a string or leave the field empty.
- Final Comment** Enter your custom text that will show up below the last data table or graph on the last page of your report. Please enter a string or leave the field empty.

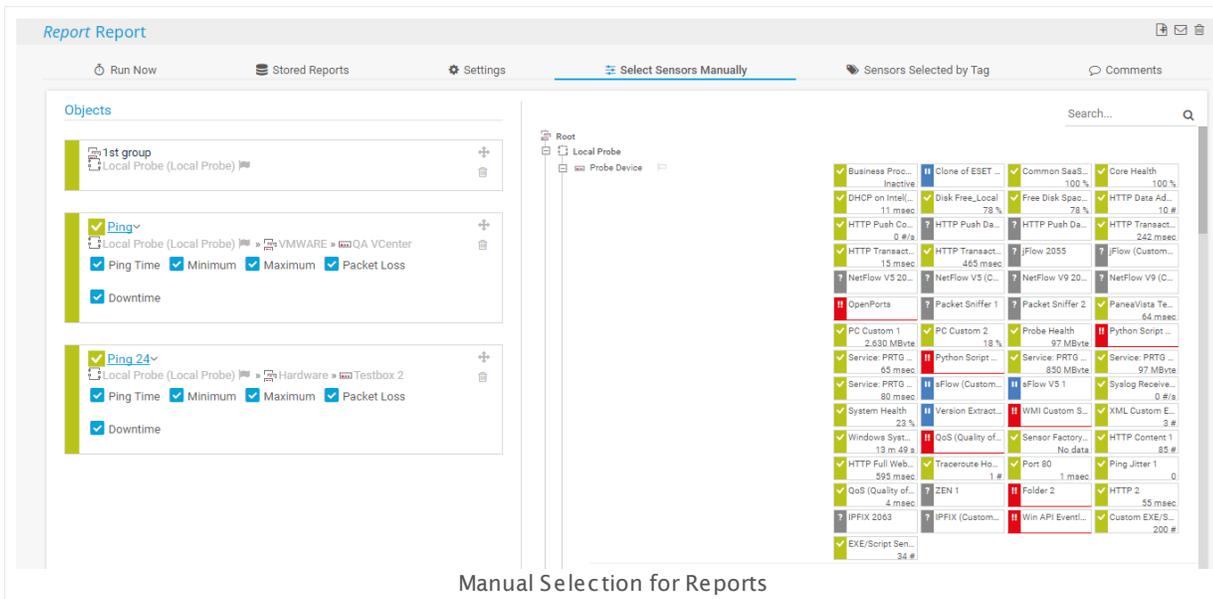
ACCESS RIGHTS

- User Group Access** Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:
- **Inherited:** Use the settings of the parent object.
 - **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
 - **Read:** Users in this group can see the object and review its settings.
 - **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
 - **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.
- You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Select Sensors Manually

Click the **Select Sensors Manually** tab to manually choose sensors that you want to include in the report. You see a split screen: On the left side, there is a list of objects that the report already contains (empty in the beginning), and on the right side, you see a less colorful view of your device tree, like on the [Management](#)^[329] tab in the device tree. You can add objects to the report using drag and drop.



▪ Add Items

From the device tree on the right side, drag objects and drop them on the list on the left side. You can add entire probes, groups, devices, or single sensors. Each dropped object is added as a new list item. Repeat this procedure as often as you wish until you have added all desired items to the report.

i The objects you drop on the left side are always added to the end of the list, you cannot add objects directly in another order.

▪ Select Sensor Channels

If you add a sensor to the selection, you can specify the sensor channels that the report will include. By default, all channels are selected. To exclude a channel from the report, remove the check mark in front of a channel name.

i If you run a PRTG [cluster](#)^[130], you can only choose between single channels if you select one specific **Cluster Node** in the report settings. If you select **All nodes** the report's **Cluster Node** setting, the channel selection is not available and the report contains only the primary channel of each sensor.

i All channels will be reselected when you move objects. We recommend that you change the order of the objects before you deselect sensor channels.

▪ Change Order

You can change the order of manually selected objects on the left side with drag and drop. Each item you add appears at the end of the list by default. To change the order, point to the drag and drop symbol (two arrows) in the upper right corner of a selected item, drag it to the desired position, and drop it there.

 All channels will be reselected when you move objects. We recommend that you change the order of the objects before you deselect sensor channels.

▪ Remove

To remove any objects from the report, click the trash can symbol next the respective list item, or select several list items while holding down the **Ctrl** key and click the green trash symbol appearing at the top of the list.

Your selection is saved automatically. There is no undo function. The final report will include both sensors selected manually and those selected by tag.

 **Permanently exclude a sensor channel from reports:** To avoid a reselection of channels when you change the object order, permanently exclude unwanted channels from the report.

1. Click the sensor name under **Objects** to open its **Overview** tab.
2. Open the [settings](#)^[3162] of the desired channel.
3. Choose option **Hide from Graphs** in section **Graph Rendering**.
4. Choose option **Hide from Tables** in section **Table Rendering**.
5. **Save** and the channel will not appear in the object selection nor in reports anymore. Note that the channel also will not appear in any other graphs or data tables using this option.

 You have to choose both hide options to not show a channel in the sensor selection of a report.

Sensors Selected by Tag

Click the **Sensors Selected by Tag** tab to view all sensors that are added to the report depending on the **Include Sensors by Tag** setting of the report. In the [table list](#)^[237], you see all sensors that you added to the report by their respective tags. This is for your information only, you cannot change sensors here.

However, you can switch to the **Settings** tab of the report and change the tags that the report uses to include sensors. Additionally, you can also exclude sensors with certain tags there. The final report will include both sensors selected manually and those selected by tag.

For sensors that you add by tag, all sensor channels are included in the report automatically, except you use a PRTG [cluster](#)^[130] and select **All nodes** in the **Cluster Node** selection of the report. In this case, the report includes only the primary channel of each sensor.

 The final report will include both sensors selected manually and those selected by tag.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: Can I change the number of PDFs created by a report?

- <https://kb.paessler.com/en/topic/11863>

Knowledge Base: How do I modify PRTG's report templates?

- <https://kb.paessler.com/en/topic/263>

Knowledge Base: How can I show full channel names below report graphs?

- <https://kb.paessler.com/en/topic/58913>
- Manual Section: [Calculating Percentiles](#) 

8.11 Maps

With the **Maps** feature (some people might call this 'dashboards') you can create web pages with up-to-the-minute monitoring status information in a customizable layout. Using this unique concept, you can also make your overview pages of live data publicly available, if you like.

Example of a PRTG Map

In this section:

- [Introduction](#) ³²⁷⁸
- [Start Maps](#) ³²⁷⁹
- [Maps Overview](#) ³²⁷⁹
- [Maps Rotation](#) ³²⁸⁰
- [Maps in Home Menu](#) ³²⁸²
- [Working with Maps](#) ³²⁸²

Introduction

There are countless possibilities for the implementation of maps. For example, you can use this feature to:

- Create network maps with status icons for each device on the map.
- Create quick views of your network that can be shown on network operations center screens.
- Create a quick network overview for publishing on the Intranet, allowing at-a-glance information for management of other employees.

- Create a custom view of the most important sensors in your monitoring setup.
- Create Top 10 lists of the sensors of a specific group or device.

Technically, a map is a usual HTML web page. You can build a schema of your network by choosing from hundreds of device icons and connect them with lines. A map can consist of the following elements:

- A set of map items, which can include device icons, sensor status icons, graphs, data tables, lists of sensors, connection lines, geographical maps, or custom HTML code.
- An optional background image (a JPG, PNG, or GIF file, for example, your company logo, or a graphical view of your network).

You can also specify the size of the map. Using the AJAX-based map editor, you can place the items anywhere on the map, and you can also change their size. Each map has a unique URL that you can use to link to the map. Users who want to access the map either need an account in your PRTG installation, or can access a public URL of the map if you allow the **Public Access** feature. Public maps contain a unique **Map ID** access key in the URL to block unwanted visitors.

PRTG comes with a pre-configured standard map that you can use right away. You can also change or delete it, if you like. The map is automatically created when you install PRTG for the first time (visible for the [PRTG System Administrator](#)^[158] user):

- **Sample Dashboard:** By default, this map shows a graphical structure of your device tree, a list of [alarms](#)^[219], a [geo map](#)^[321], and more. This sample map has a 5***** [priority](#)^[242] so you can also open it under **Home** in the [main menu](#)^[263]. To not show it in the main menu, define a lower priority.

Start Maps

Click **Maps** in the [main menu](#)^[271] to view or add custom views of your network's status and monitoring data. **Hover** over **Maps** to show other menu items. Choose between:

MAPS	
All	Open the Maps overview page where you can view or add custom views of your network's status and monitoring data.
Add Map	Open an assistant to directly add ^[326] a new map.
Select Map >	Open an existing map. Hover over Select Map to show other menu items. Follow the menu path (it is specific to your setup) to select a map.

Maps Overview

In the **All** view, you see a list of all existing maps. Click the name of a map to view it. To add a new map, hover over  and select **Add Map** from the menu.

Click the **Edit** button for the following options:

- Click the **Map Rotation** button to rotate between maps.
- Click the **Clone** button to create an exact copy of this map. As soon as you click this, the map is cloned and the cloned map's settings are shown.
- Click the **Delete** button to remove this map.
- Click the **Settings** button to edit the map settings.

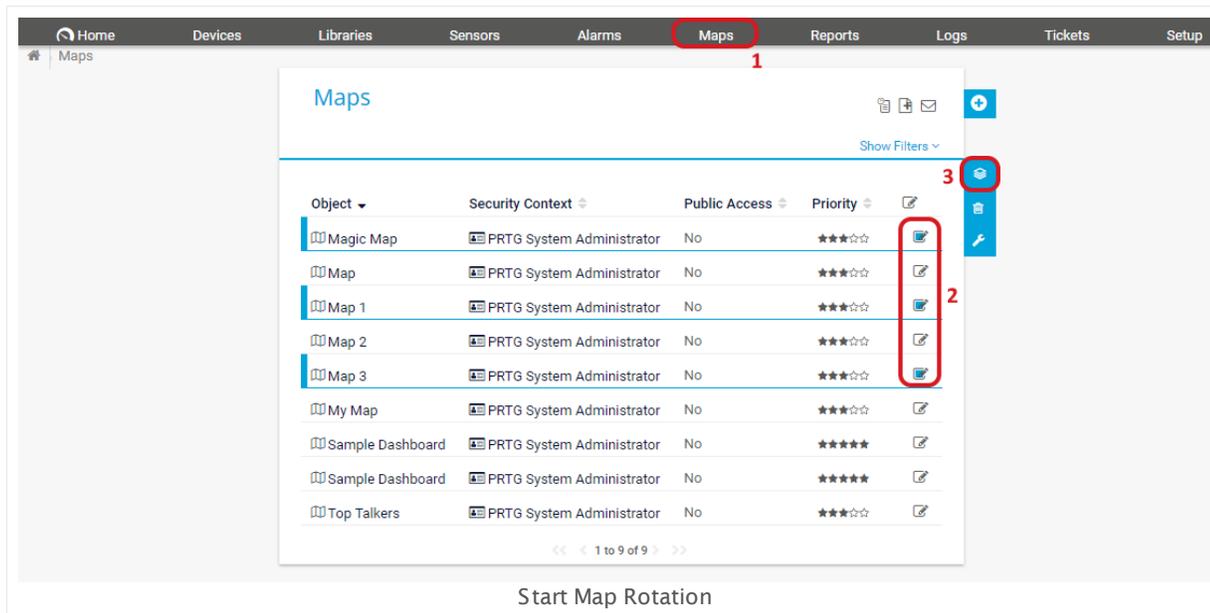
You can also define the [priority](#) of a map. Maps with a 5***** priority appear in the [main menu bar](#) under **Home** for direct selection (up to 10 entries). For details, see section [Maps in Home Menu](#).

Please also see [Working with Table Lists](#). Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the [Multi-Edit Lists](#) section.

Map Rotation

The Map Rotation feature in PRTG allows you to show several maps or dashboards rotating on one page. Map rotation makes it possible to show different information on one screen based on time. You can compare this with a slide show. Follow the steps below to configure your own map rotation.

1. Open the **Maps** overview page from the PRTG [main menu bar](#).
2. Select the maps that you want to rotate using the **Edit** buttons.
3. The [Multi-Edit](#) menu appears.
4. Click **Map Rotation** in the multi-edit menu.
5. That's all: PRTG will show the selected maps in rotation on a new page.
 This requires login credentials for PRTG.
6. You can change the time until a new map appears with the arrows symbol  in the lower right corner. Hover over the arrows symbol and choose between **10s**, **30s**, **60s** (seconds), **10m** (minutes), and **Refresh** now.



Public Map Rotation

You can also set up a **public map rotation** that you can use without login credentials. For this purpose, you have to create a custom URL that defines which maps will publicly rotate. The public map rotation URL has this format: the address of your PRTG server, followed by **/public/mapshow.htm?ids=**, followed by map IDs and secret keys.

1. Allow **public access** in the [settings](#) of the maps you want to rotate.
2. Find the map IDs and secret keys to add them to the URL that opens the public map rotation.
 - a. To find the ID of a map, open the map with your web browser. The map ID is included in the URL of the map as value of the parameter **id**, for example, `https://<yourprtgserver>/map.htm?id=2124`, where the number **2124** is the needed ID.
 - b. To find the secret key of a map, open the settings of the map, make sure you have selected a [public access option](#), and copy the entry of the **Secret Key** field.
3. Connect each map ID with the secret key of the same map using a colon, in this format: **mapid:secret key**
4. Add all IDs with their secret keys to the URL for the public map rotation. Separate each **mapid:secretkey** token from the next **mapid:secretkey** token with a comma.
5. The complete URL has this format: **https://yourprtgserver/public/mapshow.htm?ids=mapid1:secret key 1,mapid2:secret key 2,mapid3:secret key 3**
This is an example URL for public rotation of two maps:
`https://prtg.example.com/public/mapshow.htm?ids=9507:4049BEA1-B89C-4B5D-ACC4-3C8E00566EB8,9358:718D3CE1-DF00-4B92-AE8A-E0253B912C37`
6. Open the created URL with your browser and PRTG will start the public map rotation.
7. You can change the time until a new map appears with the arrows symbol in the lower right corner. Hover over the arrows symbol and choose between **10s**, **30s**, **60s** (seconds), **10m** (minutes), and **Refresh** now.

Maps in Home Menu

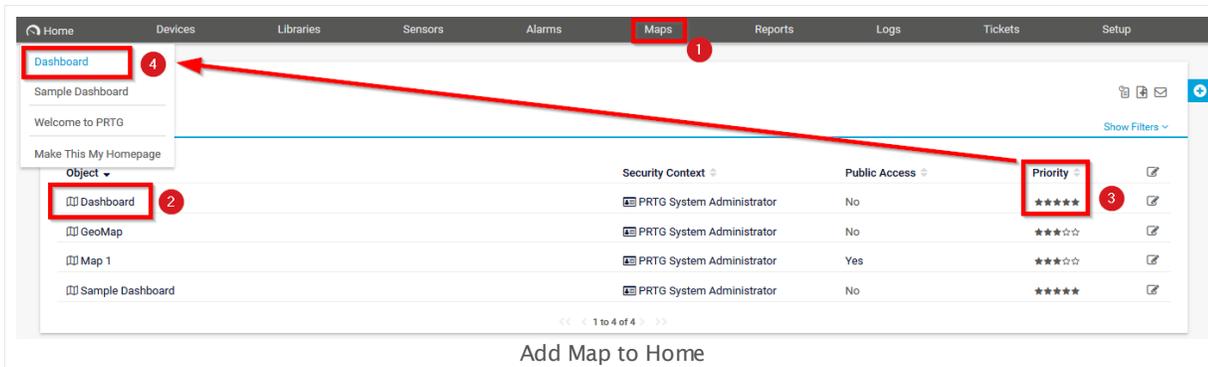
You can add any map to **Home** in the [main menu bar](#)^[263] of the PRTG web interface. This option gives you quick access to your most important maps.

If you open a map via **Home**, it will appear as **dashboard** without the [tabs](#)^[3297] that are available when opening a map via the **Maps menu**^[271]. In contrast to a map that you [open via URL](#)^[3285], your dashboard is embedded in the PRTG web interface with [global header area and page footer](#)^[181].

You can control whether a map appears in the **Home** menu via [priorities](#)^[242]. Every map with a 5***** star priority will appear as a single entry under **Home**. You can include up to 10 map entries in the **Home** menu.

1. Open the **Maps** overview via the PRTG [main menu bar](#)^[271].
 2. In the [table list](#)^[237], look for the entry of the map that you want to add to the **Home** menu.
 3. In column **Priority**, select 5***** stars for the desired map.
- ✔ The map will appear in the **Home** menu (manually refresh the page with **F5** to immediately see the changes).

❗ PRTG provides a sample dashboard in the **Home** menu by default. You can remove the sample dashboard and other, later defined dashboards from the menu by changing the priority to 4***** stars or lower.



Working with Maps

For detailed information on how to create and edit maps, and to learn how to make them accessible to others, see the following sections.

- [Maps Step By Step](#)^[3283]
- [Map Designer](#)^[3287]
- [Maps Other Settings](#)^[3297]

8.11.1 Maps Step By Step

To create a new map, follow the steps in this section. In the web interface, click **Maps** in the [main menu bar](#)³²⁸³ to show the maps main screen.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

In this section:

- [Step 1: Add Map](#)³²⁸³
- [Step 2: Add Map Items](#)³²⁸⁴
- [Step 3: View and Share](#)³²⁸⁵
- [Create Advanced Maps](#)³²⁸⁵

Step 1: Add Map

Hover over  and select **Add Map** from the menu to add a map. An assistant appears. Enter a **Map Name** and define **Map Layout** settings (size and optionally a background image). In the **Public Access** section, define the accessibility to your map without login.

 For detailed information, see [Maps Settings](#)³²⁹⁷ section (Settings).

Add Map (Step 1 of 2)

< Cancel

Map Name

Map Name ⓘ

Map

Map Layout

Map Width ⓘ

800

Map Height ⓘ

600

Background Image (optional) ⓘ

Select File

Public Access

Allow Public Access ⓘ

No public access (map cannot be viewed without login)

Allow public access (map can be viewed by using a unique URL)

Allow public access, disable all links (map can be viewed by using a unique URL)

Create 

Add Maps Assistant Step 1

Step 2: Add Map Items

- Click the **Create** button to open the **Map Designer**.
- Select an object from the device tree on the left.
- **Drag&drop** an object from the items list on the right to the main window of the Map Designer.
- The item will immediately appear on the map.
- Define further properties of the item: mark it in the main window of the Map Designer and see section **Properties** on the right. **Save** your changes to the properties.

- Repeat this procedure as often as you wish until you have added all desired items to the map.
- Drag items to change their position. You can also draw connection lines between items and edit the properties of existing items.

 For detailed information, see [Map Designer](#)³²⁸⁷ section.

Step 3: View and Share

Click the **View Map** tab to see your map. If available for an object, you can click most object names as well as all sensors. It depends on the access rights of the object and the currently logged in user account if you can get more detailed information about the object or an error message indicating insufficient access rights.

Click the **Get HTML** tab to get the direct URL of your map that you can share with others. You can also [add your map as dashboard to the Home menu](#)³²⁸² of the PRTG web interface.

 For detailed information, see [Maps Settings](#)³³⁰⁰ section.

-  The single map items will refresh in the refresh interval you define for this map when viewing it. Hover over the arrows symbol in the lower right corner to define the interval.
-  Map objects of type **Data Tables**, for example, include entries according to the security context as defined in the [settings of the map](#)³²⁹⁷, but the table headings regard to the rights of the particular user account that views the map. Because of this, a user might see more objects in the table itself than denoted in the header.

Create Advanced Maps

PRTG Maps provide the possibility to publish data from various sources. Besides using the default map items you can create a completely individual map with desired data in any design. See the following articles for more details.

- **Adding External Information to PRTG Maps:** <https://kb.paessler.com/en/topic/9263>
Embed information from other sources than PRTG into your map using IFRAME or IMG, for example, weather and traffic maps or webcam images.
- **Map Rotation and Public Map Rotation:** [PRTG Manual: Maps](#)³²⁸⁰
Show several maps rotating on one page just like in a slide show.
- **Nest Maps:** <https://kb.paessler.com/en/topic/71833>
Display and link multiple maps within one map.
- **Accumulating Sensor Data with HTTP XML/REST Value Sensor:** <https://kb.paessler.com/en/topic/71932>
Display sensor data from various PRTG installations in a single map using the [HTTP XML/REST Value sensor](#)¹⁰⁹⁵.
- **Use your Own Images in PRTG Maps:** <https://kb.paessler.com/en/topic/8043>
Add any browser-compatible image to your map.
- **Adding and Customizing Map Objects:** <https://kb.paessler.com/en/topic/1703>
Create customized or completely new map objects.

Part 8: Ajax Web Interface—Advanced Procedures | 11 Maps
1 Maps Step By Step

- **Custom Map Objects for PRTG Maps:** <https://kb.paessler.com/en/topic/61263>
Find ready-to-use custom map objects and other map customizations.

More

Video Tutorial: How to Create Maps in PRTG

- <https://www.paessler.com/support/videos/prtg-advanced/creating-maps>

8.11.2 Map Designer

Use the **Map Designer** to create a map web page representing your network.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

In this section:

- [Use a Proper Browser](#)  3287
- [Basic Design Concept](#)  3287
- [Device Tree Selection](#)  3288
- [Properties Selection](#)  3290
- [Edit Existing Map Items—Properties Box](#)  3293
- [Edit Existing Map Items—Hover Icons](#)  3294
- [Edit Existing Map Items—Using Cursor Keys](#)  3294
- [Draw Connection Lines Between Items](#)  3294
- [Snap To Grid](#)  3295
- [Undo and Redo](#)  3296
- [More](#)  3296

Use the Proper Browser

Due to the map designer's extensive scripting capability, it is important that you use a compatible browser when editing maps. We recommend that you use Google Chrome 67 or later (recommended). You can also use Mozilla Firefox 61 or later, or Microsoft Internet Explorer 11. The map designer is **not** fully compatible with earlier versions of Internet Explorer or Opera browsers.

Basic Design Concept

Click the **Map Designer** tab to open the editor. It might take a few moments to load. Here, you can create your map by adding or changing items. The designer screen consists of three main parts: The **Device Tree** on the left side, the current **Map** in the middle, and the **Properties** on the right side.

Part 8: Ajax Web Interface—Advanced Procedures | 11 Maps 2 Map Designer

The screenshot displays the PRTG Network Monitor Map Designer interface. On the left is the 'Device Tree' with a search bar and a list of nodes including 'HQ (Local Probe)', 'AWS', 'Probe Device', and various sensors like 'Core Health', 'CPU Load Loc', 'Probe Health', 'System Health', 'Logins Failed', 'Windows Syst', 'Sensor Count', 'QoS One Way', 'Volume IO Tc', 'Volume IO C:', 'Volume IO Ha', 'PRTG user Lo', 'Planty 4 - Soil', 'Planty 1 - Soil', and 'Planty APAC'. The central map area features a large 'PRTG NETWORK MONITOR' logo, a donut chart titled 'Top 10: Most Used CPUs (Branch Office (Remote Probe))' with a value of 3525, and a central icon of a server rack labeled 'HQ (Local Probe)'. The donut chart is divided into segments representing different sensors. The 'Properties' panel on the right shows 'Default Icons A' and 'Default Icons B' with various icon sets, and a list of sensors including 'CPU Load', 'SNMP CPU Load', and 'System'. The interface also includes a 'View Map' button, 'Map Designer' tab, 'Settings', 'Get HTML', 'Comments', and 'History' options.

Each map item takes attributes from both selections.

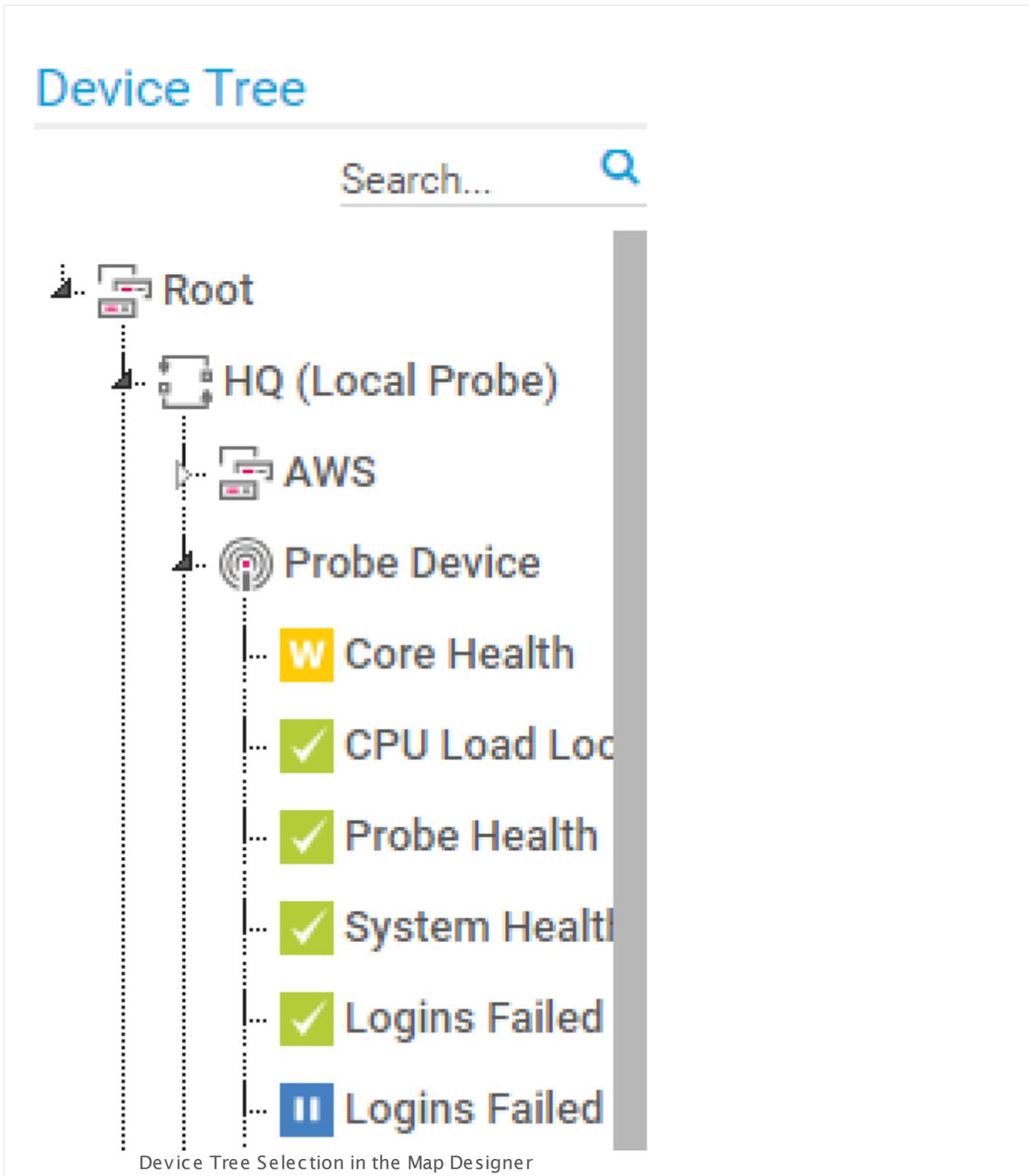
- **Device Tree** (left): Select the monitored object whose data you want to show on the map.
- **Properties** (right): Define how to show the map item.

Simply **drag&drop** any object from either side onto the map, or **double-click** on an object. You will always see all changes immediately.

Device Tree Selection

Use the **Device Tree** to select the monitored object whose data you want to show on the map (this can be a probe, a group, a device, or a single sensor). To find the desired object you have the following options:

- Use the arrow symbols at the beginning of each line to open nodes in the device tree and show objects below probes, groups, and devices.
- Enter a few characters into the **Search** box in the upper right corner to search for names (or part of names) of objects in your configuration. You will see the search results immediately. Click the gray x icon to clear your search.



- No matter which method you choose to find the desired object, you can always drag any object from the **Device Tree** onto a free area of the map to create a new map item.
- If you drag it onto an existing map item, it replaces the existing item while **Properties** and size stay the same.
- You can also select a map item and double click a **Device Tree** object to replace the map item. If no item is selected, double clicking an object adds a new map item.

- To gain more space for map editing, reduce the size of the **Device Tree** box by dragging its right border to the left. Drag it to the right to enlarge it again.

Properties Selection

Use the **Properties** selection to define how to show the map item (for example, as an icon, a map, a table, or a graph). Select the appearance in different categories. Hover over a property object to get a live preview of it (in most cases).

- ① If a certain **Properties** object is not available for the selected **Device Tree** object, you will see a corresponding text note.

Properties

Top:	Left:	Width:	Height:	Layer:
100	50	350	460	2

External Link: [Select object](#)

HTML Before:

HTML After:

- > Default Icons A
- > Default Icons B
- > Icons A
- > Icons A (Static)
- > Icons B
- > Icons B (Static)
- > Icons C
- > Icons C (Static)
- > Static Images
- > Status Icons
- > Cluster
- > Data Tables
- > Device Tree Views
- > Status Donuts
- > Geo Maps
- > Graphs
- > Objects
- > Top 10
- > Custom HTML

Properties Selection in the Map Designer

There are many different property object types available. Simply click one of the categories to show all available types.

- **Default Icons A, Default Icons B**

These categories offer a variety of iconic symbols of typical network devices in the current PRTG style. Category A comes with object data which category B does not include.

- **Icons A, Icons B, Icons C**

These three categories offer a variety of iconic symbols of typical network devices. Below each icon you can see the object name and a sensor overview for the object. This shows how many sensors are in which [status](#)^[195]. For some sensors, a mini graph is shown as well.

- **Icons A (Static), Icons B (Static), Icons C (Static)**

These three categories offer the same variety of iconic symbols of typical network devices as the category described above. Here, no object data is displayed but only the icon.

- **Static Images**

This category offers free or public domain geographical maps from different sources. Use properties section Geo Maps if you want to show PRTG [Geo Maps](#)^[321] in the map.

 The items in this section are independent from the selected **Device Tree** objects.

 For additional geographical maps and other map customizations, see this Knowledge Base article: [Where can I find custom map objects and other map customizations?](#)

- **Status Icons**

This category offers options to insert [status](#)^[195] icons in different styles. These show the object name and an overview of how many sensors there are and their status. For example, you can add "traffic lights" or the QR code of a monitoring object to your map. There is also an object available for audible alert that will play a sound when the number of alarms of the monitored object are > 0. Note that your browser must support playing embedded sounds for this icon.

 See also this Knowledge Base article: [Which audible notifications are available in PRTG? Can I change the default sound?](#)

- **Cluster**

If you use the PRTG [Clustering](#)^[130] feature, you can add icons to your map that show the status of your cluster.

 The **Map** icon does not scale automatically, so the nodes are displayed on top of each other by default. Please manually enlarge this icon in the main window of the **Map Designer** (downwards and to the right) until it fits your needs.

- **Data Tables**

Choose from several [table lists](#)^[237] that show sensor lists for the currently selected object. You can also choose from several lists that show sensors in a certain status only.

- **Device Tree Views**

Add several [views of your device tree](#)^[187] to the map, including [sensor gauges](#)^[198] for the selected object.

- **Status Donuts**

Choose from several status donuts that either show all alarms or all sensor states for the selected object. These are the same status donuts that you see on the [Welcome Page](#)^[175].

- **Geo Maps**

In this category you can choose between a globe and a geographical map. You can see the location of the currently selected object in the **Device Tree** on the map. To use this feature, you must enable Geo Maps integration and you have to enter a **Location** in the settings of the monitoring object you want to use this with. For more information, see the [Geo Maps](#)^[321] section.

 If Geo Maps integration is disabled, you will only see white boxes instead of map previews.

- **Graphs**
This category offers different graph styles in several dimensions and detail. You can also select graphs including a legend or sensor states.
- **Objects**
Add some simple geometric shapes to your map. The items in this section do not depend on the selected object in the **Device Tree**.
- **Top 10**
Choose from several tables that show the top 10 sensors in certain categories, like least used CPUs, highest bandwidth usage, best availability, or slowest websites.
- **Custom HTML**
You can use this property, for example, to add [custom text](#)³²⁹⁴, external images or applets to your map. To actually add custom HTML code to your map, add the item, and mark it to [edit](#)³²⁹³. You can then copy your custom code into the **HTML Before** and **HTML After** fields in the **Properties** box on the right side.

No matter which object you choose, you can always drag any object from the **Properties** box onto a free area of the map to create a new map item. If you drag it onto an existing map item, it replaces this item, while its **Device Tree** object attributes and size stay the same. You can also select a map item and double click an object in the **Properties** box to replace the map item. If no item is selected, double clicking an object will add a new map item.

To gain more space for map editing, reduce the size of the **Properties** box by dragging its left border to the right. Drag it to the left to enlarge it again.

Edit Existing Map Items—Properties Box

Click a map item to select it. You can then edit its attributes using the fields in the upper part of the **Properties** box on the right side:

- **Top, Left, Width, and Height** fields
Enter position and size values for direct positioning. Click the **Save** button to save your settings. Alternative: Use the mouse to move and resize a map item.
- **Layer** field
The layer number defines if an item appears on top of or behind another item if they overlap. The item with the higher number appears on top. Enter a positive integer value and click the **Save** button to save your settings. Alternative: Use the arrow symbols in the context menu of a map item to **Bring to front** or **Send to back** an item one layer (see below).
- **External Link**
PRTG maps are interactive. You can enter the address of any website here. If you click the map item when viewing the map, PRTG will open this page in a browser window. Enter the whole URL to an external website (for example, <https://www.paessler.com>) or the address of a subpage of your PRTG installation (for example, [devices.htm](#)).
- **HTML**
Click the arrow symbol underneath to show the **HTML Before** and **HTML After** fields. Any HTML code you enter in these fields is added before or respectively after the map item. Enter your custom HTML code that embeds an object and click the **Save** button. Your HTML object is inserted into the map. For example, you can enter the code `` to insert an image of a Paessler logo.

Edit Existing Map Items—Hover Icons

Hover over a map item to show the edit icons for it.

- **Bring to front (arrow up symbol)**
Move this item one layer to the front. This is useful when adding several items to a map that overlap each other.
- **Send to back (arrow down symbol)**
Move this item one layer to the back. This is useful when adding several items to a map that overlap each other.
- **Delete (trash symbol)**
Delete this item.
 Be careful! The item will be deleted immediately without notice and you cannot undo this. Alternative: Select the item and press the **Del** button on your keyboard.
- **Drop Connections (scissors symbol)**
If there are connection lines between two items, you can delete all lines starting from this item. Connection lines will be dropped immediately.

Edit Existing Map Items—Using Cursor Keys

While an object is selected, use the cursor keys to move it one pixel at a time. Hold the **Shift** key in combination with the cursor keys to move the object 10 pixels at a time.

Add Custom Text to the Map

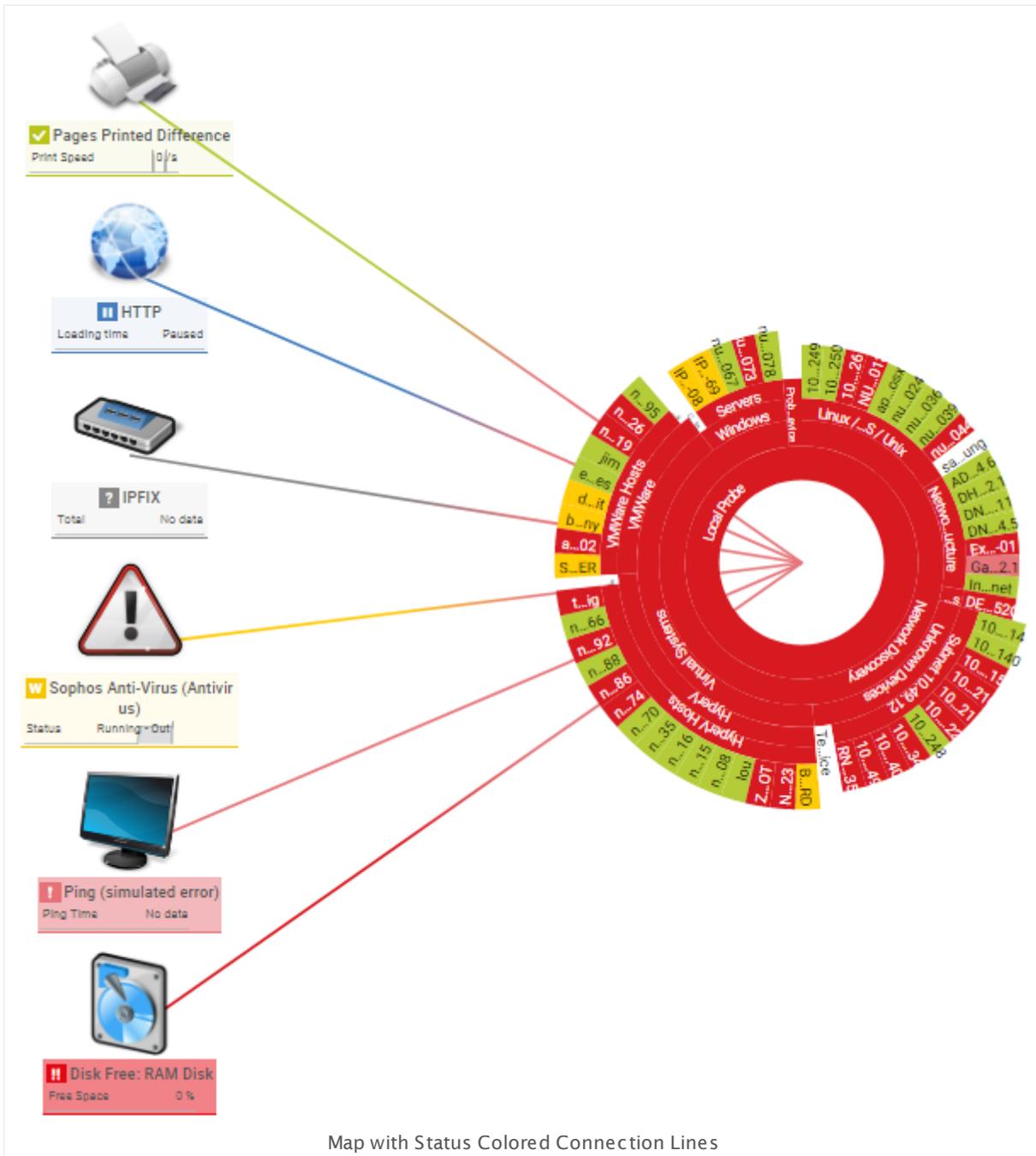
You can add custom text with individual styling to your map using the **Custom HTML Element**.

 For details, see the Knowledge Base: [How to add text to a map?](#)

Draw Connection Lines Between Items

You can draw connection lines between any map items via drag and drop. Click the gray handles next to an item and drag a line to the item you want to draw a connection to. A line between these items appears immediately. This can be useful to indicate network connections or logical coherence between two items. To delete connection lines, click the scissors symbol in the item's [edit icons](#)³²⁹³.

Lines between objects are colored dynamically depending on the [status](#)¹⁹⁵ of linked objects. For example, a line is red as long as one of the object's icons shows a red **Down** status. This only affects half of the line, at the end where the red sensor is shown. If both objects connected show a red sensor, this results in a continuous red line.



Snap to Grid

Choose **Snap to Grid** below the **Device Tree** box to define how map items are positioned when adding or moving them via drag and drop. The setting is active immediately. With snap to grid enabled, you can place items aligned with the grid only. If you deselect the **Snap to Grid** option, you can place map objects completely free.

Undo and Redo

You can revert previous changes to the map and its objects with the **Undo** button (**Ctrl+Z**) in the **Device Tree** box. To revert undo actions, use the **Redo** button (**Ctrl+Y**). You can undo and redo up to 50 changes when you work on a map. Because PRTG saves changes persistently in your configuration, you can even revert changes later.

Both buttons are only available if they can apply, otherwise they are grayed out.

More

Knowledge Base: Why does my browser show an unresponsive script warning while loading the Map Designer?

- <https://kb.paessler.com/en/topic/19483>

Knowledge Base: How can I add or edit map objects used for PRTG's maps?

- <https://kb.paessler.com/en/topic/1703>

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <https://kb.paessler.com/en/topic/26303>

Knowledge Base: Where can I find custom map objects and other map customizations?

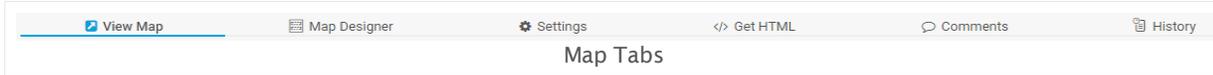
- <https://kb.paessler.com/en/topic/61263>

Knowledge Base: How to add text to a map?

- <https://kb.paessler.com/en/topic/11523>

8.11.3 Maps Settings

Using the Map tabs you can access all functionalities and settings for a map.



View Map

Click the **View Map** tab any time to show a preview of your map.

Map Designer

Click the **Map Designer** tab to edit the contents of your map.

 For details, see manual section [Map Designer](#)³²⁸⁷.

Settings

Click the **Settings** tab to open a map's general settings.

 When using the **Add Map** dialog, not all of these settings are available. You can change them later by clicking the **Settings** tab.

BASIC MAP SETTINGS

Map Name	Enter a meaningful name for the map.
Security Context and Color Mode	<p>Define the user account that the map will use for access to monitoring data. The map will only contain objects that the selected user¹⁵⁸ is allowed to view. This setting also affects the color mode³³⁰⁷ of maps that are displayed without a PRTG login (public maps). In this case, the color mode setting from the security context user is taken.</p> <p>Choose a user account from the list. The available users depend on your configuration. By default, the security context is the user account that created the map. PRTG System Administrator users can change this setting.</p> <p> Basically, the security context is the minimum access right a user account has when viewing a map. If the security context of a map is PRTG System Administrator, every user account will see all objects on the map, no matter what the particular user rights are.</p>

BASIC MAP SETTINGS

i Map objects of type **Data Tables**, for example, include entries according to the security context, but the table headings regard to the rights of the particular user account that views the map. Because of this, a user might see more objects in the table itself than denoted in the header.

Timezone Define the time zone that the map will use for all date-specific options. Select a time zone from the list.

Tag Filter This setting affects table map objects. Enter one or more tags separated by spaces or commas to include sensors in tables. Only sensors with one of the tags entered here will appear in this map's data tables, including sensors that [inherit](#)¹³⁷ tags from parent objects. Please enter a string or leave the field empty.

i For some map objects like sunburst and treemap, the tag filter applies to devices, groups, and probes. If you use only tags of sensors, these map objects will not appear on the map. Filtering sunburst and treemap objects with multiple tags may not work properly and is not officially supported.

i Use this setting with care because it will affect all tables of the current map!

MAP LAYOUT

Map Width Define the width of the map in pixels. Please enter an integer value.

Map Height Define the height of the map in pixels. Please enter an integer value.

Automatic Scaling Define if you want the map to automatically adapt to your screen size. Choose between:

- **Scale map view to fit browser size:** The size of the map adapts automatically to the size of your screen. Choose this method if the map is shown on various screens with different resolutions so that it uses the available place in the browser window the best possible way.
- **Do not auto-scale map view:** The map uses always the size that you define above.

MAP LAYOUT

Background Picture	<p>Define if you want to use a background picture for the map. Choose between:</p> <ul style="list-style-type: none">▪ Use an image in the background of the map: Use a custom background image that you define below.▪ Do not use a background image: Do not use a background image.
Background Image	<p>This option is only visible if you enable a background picture above. Click the Select File button and select an image from your computer or network.</p> <p> Only images in the format JPG, PNG, and GIF are supported. The file size must be smaller than 20 MB. If you try to upload other images, you get an error message.</p>
Background Color	<p>Select a background color for this map. Either enter a hex color code or choose a color from the color selector. The hex color code field will always display the currently defined color.</p>

PUBLIC ACCESS

Public Access	<p>Define if others can see the map. Choose between:</p> <ul style="list-style-type: none">▪ No public access (map cannot be viewed without login): Do not allow public access to the map. Only users with both a login to the PRTG web interface and sufficient access rights can see the map.▪ Allow public access (map can be viewed by using a unique URL): Allow access to the map using a unique address. The URL contains a key that you can change below. The map will be an interactive public map.▪ Allow public access, disable all links except for Geo Maps (map can be viewed by using a unique URL): Allow access to the map using a unique address. The URL contains a key that you can change below. If you choose this option, all links on the map are disabled, so it will be a non-interactive public map.  This option does not apply to geographical maps  embedded in your map. It is not possible to disable the links in map objects that contain a Geo Map. Workaround: Place an empty, transparent square object over the Geo Map object and link it to an unrelated URL.
---------------	---

PUBLIC ACCESS

i Maps with public access are displayed using the color mode from the security context user. See Security Context and Color Mode for more information.

Secret Key

This field is only visible if public access is enabled above. The key is automatically generated. It is part of the public URL for the map. You can also enter a customized string. We recommend that you use the default value. For more information on public access, see the [Get HTML](#)³³⁰⁰ section.

i The characters comma "," and colon ":" are not allowed in the secret key field!

ACCESS RIGHTS

User Group Access

Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
- **Read:** Users in this group can see the object and review its settings.
- **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the [System Administration—User Groups](#)³³⁸³ settings.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Get HTML

Your PRTG map is like a standalone HTML page. You can make it accessible to others, if you like. Depending on the **Public Access** [setting](#)³²⁹⁷ of your map, a visitor needs to provide PRTG user account login data to view the map, or sees the map immediately using a URL containing a secret key. When using this unique key, you can also include your map on another webpage, embedding it via `<iframe>`.

- **Option 1: Link to a web page with the map that requires login credentials**
The shown URL requires login credentials in order to display the map. PRTG asks the user trying to view the map via this URL for login credentials.
 - ❗ In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.
- **Option 2: Link to a web page that displays the map without a login**
To get the shown URL working for public access without a login, enable **Public Access** in the [settings tab](#)³²⁹⁷ of your map.
 - ❗ In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.
- **Option 3: Show a map inside other web pages using an IFRAME**
For your convenience, this shows source code for adding an **iframe** to another webpage. It includes a URL for direct access. Just copy the code and paste it into your webpage code. Also enable **Public Access** in the [settings tab](#)³²⁹⁷.
 - ❗ In the URL, usually the IP address is given via which the page is available. Maybe a NAT translation is set in your firewall, or you may want to use a domain name or a name from a dynamic DNS service for public access. Please customize the URL you use for access to your needs.

While a map is shown via these URLs, you can change the refresh interval any time by hovering over the arrows symbol in the lower right corner. Choose between **10**, **30**, or **60** seconds, **10** minutes or **Refresh** now. The map adapts automatically to the size of the browser window if you enable the [auto-scaling setting](#)³²⁹⁷.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Delete

You can delete the entire map any time by clicking the trash symbol on the right.

More

PRTG Manual:

- [Data Reporting](#)¹⁶²

8.12 Setup

In the setup settings of the PRTG web interface, you can define almost all system settings for PRTG. However, some of the machine-oriented settings are defined using two Windows administration tools (see [Others](#)³³⁰³ section below).

In the main menu, click on **Setup** to show the available options.

- Some setup options are only available for PRTG on premises (marked with the PRTG on premises icon), so you cannot use these on PRTG hosted by Paessler instances.
- ☁ Some setup options are only available for PRTG hosted by Paessler (marked with the PRTG hosted by Paessler icon), so you cannot use these on PRTG on premises instances.

PRTG Status

- [PRTG Status—System Status](#)³³⁹⁶
- [PRTG Status—Cluster Status](#)³⁴¹² ■
- [PRTG Status—Licensing Status and Settings](#)³⁴¹⁴ ■
- [PRTG Status—Auto-Update](#)³⁴⁰⁷ ■

Account Settings

- [Account Settings—My Account](#)³³⁰⁴
- [Account Settings—Notification Templates](#)³³¹¹
- [Account Settings—Notification Contacts](#)³³³⁴
- [Account Settings—Schedules](#)³³³⁶

System Administration

- [Manage Subscriptions](#)⁷¹ ☁
- [System Administration—User Interface](#)³³⁴³
- [System Administration—Monitoring](#)³³⁵⁵
- [System Administration—Notification Delivery](#)³³⁶¹
- [System Administration—Core & Probes](#)³³⁶⁶
- [System Administration—User Accounts](#)³³⁷⁶
- [System Administration—User Groups](#)³³⁸³
- [System Administration—Administrative Tools](#)³³⁸⁸
- [System Administration—Cluster](#)³³⁹⁴ ■

Optional Downloads and Tools

- [Downloads and Tools—Client App for Windows \(Enterprise Console\)](#)  
- [Downloads and Tools—Client Apps for Mobile Devices](#) 
- [Downloads and Tools—Remote Probe Installer](#) 

Support

- [Support—Contact Support](#) 

Others

There are some settings that you have to make in the [PRTG Administration Tool](#) , running as Windows application.

-  For more details, see sections [PRTG Administration Tool on Core Server System](#)  and [PRTG Administration Tool on Remote Probe System](#) .

8.12.1 Account Settings—My Account

In the **My Account** settings you can define values regarding your (currently logged in) PRTG user. All settings in this section are user-specific. Some account options may not be available, but restricted to the administrator.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

The screenshot shows the 'Account Settings' page for a user. The page has a navigation bar with 'My Account', 'Notification Templates', 'Notification Contacts', and 'Schedules'. The main content area is divided into three sections:

- Mobile App:** Includes a 'Use Mobile App' checkbox and a 'Show QR Code for Mobile App Login' button.
- User Account:** Contains input fields for 'Login Name' (prtgadmin), 'Display Name' (PRTG System Administrator), and 'Primary Email Address' (johnqpublic@company.com). There is a 'Save' button. The 'Password' section has radio buttons for 'Don't change' (selected) and 'Specify new password'. There is also a 'Passhash' field with a 'Show passhash' button.
- Account Control:** Includes a 'Primary Group' dropdown menu (set to 'PRTG Administrators'), a 'Status' field (set to 'Active'), and a 'Last Login' timestamp (25.07.2018 10:41:38).

The page footer reads 'My Account Settings'.

My Account Settings

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

MOBILE APP

Use Mobile App

Click **Show QR code for Mobile App Login** to display the QR code to easily copy your account settings to the mobile app.

USER ACCOUNT

Login Name

Enter the login name for the user.

 This option is not available in PRTG hosted by Paessler.

Display Name

Enter a name that the user recognizes. It will not be used for login purposes.

Primary Email Address

Enter the user's email address.

 Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG.

Password

Define the user password. For security reasons, the account settings page does not contain the password. Choose between:

- **Don't change**
- **Specify new password**

If you choose to specify a new password, enter the old password and then the new password twice.

 The new password must be at least 8 characters long. It must contain a number and a capital letter. Leading and trailing whitespaces will be cut. The password of a PRTG Administrator user can only be changed by the same PRTG Administrator user.

 This option is not available in PRTG hosted by Paessler.

Passhash

Click **Show passhash** to display the passhash for the selected user. You need the passhash of a user if you use the PRTG [Application Programming Interface \(API\)](#)³⁸⁰⁶. This setting is shown for your information only and cannot be changed here.

 This option is not available in PRTG hosted by Paessler.

API ACCESS

 These settings are only available in PRTG hosted by Paessler.

API Username	Shows the username of the current user account. You need a username if you use the PRTG Application Programming Interface (API) ³⁶⁰⁶ . This setting is shown for your information only and cannot be changed here.
API Passthrough	Click Show passthrough to display the passthrough for the selected user. You need the passthrough of a user if you use the PRTG Application Programming Interface (API) ³⁶⁰⁶ . This setting is shown for your information only and cannot be changed here.
Reset API Passthrough	Click Generate new passthrough to reset the passthrough of the current user.

ACCOUNT CONTROL

Account Type	<p>This setting is only visible to administrator users. However, it will not show if the user whose account you want to modify is a member of a group with administrative rights.</p> <p>Define the account type for the current user. Choose between:</p> <ul style="list-style-type: none">▪ Read/Write User: You can change settings.▪ Read Only User: You cannot edit any settings except your own password. This is a good choice for public or semi-public logins. <p> This setting cannot be changed for the default administrator user.</p>
Acknowledge Alarms	<p>This setting is only visible if Read Only User is enabled above. Acknowledging an alarm is an action that requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms²²⁰. Choose between:</p> <ul style="list-style-type: none">▪ User may acknowledge alarms: Allow acknowledging alarms for this user.▪ User may not acknowledge alarms (default): The user will not be able to acknowledge alarms.

ACCOUNT CONTROL

Password Changes	<p>Decide if you want the user to be able to change their account's password or not. If you allow the user to change the password, this option will be available in the My Account settings of the respective user. Choose between:</p> <ul style="list-style-type: none">▪ User may change the account password▪ User may not change the password (default) <p> This field is only visible if you edit this option for read-only users as an administrator.</p>
Primary Group	<p>This setting is available only for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience there is no difference between the primary and other user groups.</p> <p> You cannot change the primary group of Active Directory users. Users that you added with Active Directory Integration can only have this AD group as their primary group. If you need to change this, please delete this user account and add it again.</p>
Status	<p>This setting is only shown for administrator users. Define the status of the current user. Choose between:</p> <ul style="list-style-type: none">▪ Active: The current user can login to the account.▪ Inactive: The current user's login is disabled. Use this option to temporarily deny access for this user. <p> This setting cannot be changed for the default administrator user.</p>
Last Login	<p>Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.</p>

USER GROUPS

Member of	<p>Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.</p>
-----------	---

WEB INTERFACE

Auto Refresh	<p>Define if you want PRTG to reload web pages automatically for the current user. Choose between:</p> <ul style="list-style-type: none">▪ Refresh pages (recommended): Automatically refresh the single page elements on the web pages in PRTG.▪ No automatic refresh: Do not automatically refresh web
Auto Refresh Interval (Sec.)	<p>This setting is only relevant if you enable auto refresh above. Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use 30 seconds or more. Minimum value is 20 seconds.</p> <p> Shorter intervals create more CPU load on the server running PRTG. If you experience load problems while using the web interface (or PRTG maps³²⁷⁸), please set a higher interval.</p>
Play Audible Alarms	<p>Define when PRTG will play an audible alarm the current user on web pages whenever there are new alarms²¹⁹. Choose between:</p> <ul style="list-style-type: none">▪ Never: Do not play sound files on any web pages.▪ On dashboard pages only: When there are new alarms, play a predefined sound on dashboard²⁶³ pages only. The sound will be played with every refresh of the dashboard page if there is at least one new alarm.▪ On all pages: When there are new alarms, play a predefined sound on all web pages. The sound will be played with every page refresh if there is at least one new alarm. <p> Audible alarms are only played if the New Alarms value in the Global Header Area¹⁸³ of the PRTG web interface is greater than 0 after a page refresh. The number of existing alarms is not considered.</p> <p> For more information about audible notifications and supported browsers, see this Knowledge Base article: Which audible notifications are available in PRTG? Can I change the default sound?</p>
Homepage URL	<p>Define the user's default page, which is loaded after logging in or clicking on the Home²⁶³ button in the main menu.</p>
Timezone	<p>Define the time zone for the current user. Depending on the time zone you select here, PRTG shows the current user's local time zone in all data tables and graph legends.</p> <p> PRTG receives the UTC (Coordinated Universal Time) from the system time set on the PRTG core server for this purpose.</p>

WEB INTERFACE

Date Format	<p>Define the date format for the current user. The following formats are available:</p> <ul style="list-style-type: none">▪ Use System Settings: Use the date format of the server PRTG runs on.▪ DD.MM.YYYY HH:MM:SS (24h)▪ DD.MM.YYYY HH:MM:SS (AM/PM)▪ MM/DD/YYYY HH:MM:SS (24h)▪ MM/DD/YYYY HH:MM:SS (AM/PM)▪ YYYY-MM-DD HH:MM:SS (24h)▪ YYYY-MM-DD HH:MM:SS (AM/PM) <p> This setting will take effect after the next login.</p>
Color Mode	Select a color mode for your web interface.

TICKET SYSTEM

Email Notifications	<p>Define if you want to get emails from the ticket system. Choose between:</p> <ul style="list-style-type: none">▪ I want to receive an email whenever a ticket changes: You will receive an email each time a ticket is assigned to you or your user group, or if a ticket that is assigned to you or your user group is changed.  If you edit tickets that are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email.▪ I do not want to receive any emails from the ticket system: You will not get any emails about tickets.
---------------------	---

Notification Contacts

In the [Notification Contacts](#)³³³⁴ tab you can define recipients for each user account. Recipients can be email addresses, phone numbers, or push devices (iOS and Android devices with the corresponding [PRTG smartphone app](#)³⁴⁰⁴).

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Save your settings. If you leave the current page, all changes to the settings will be lost!

More

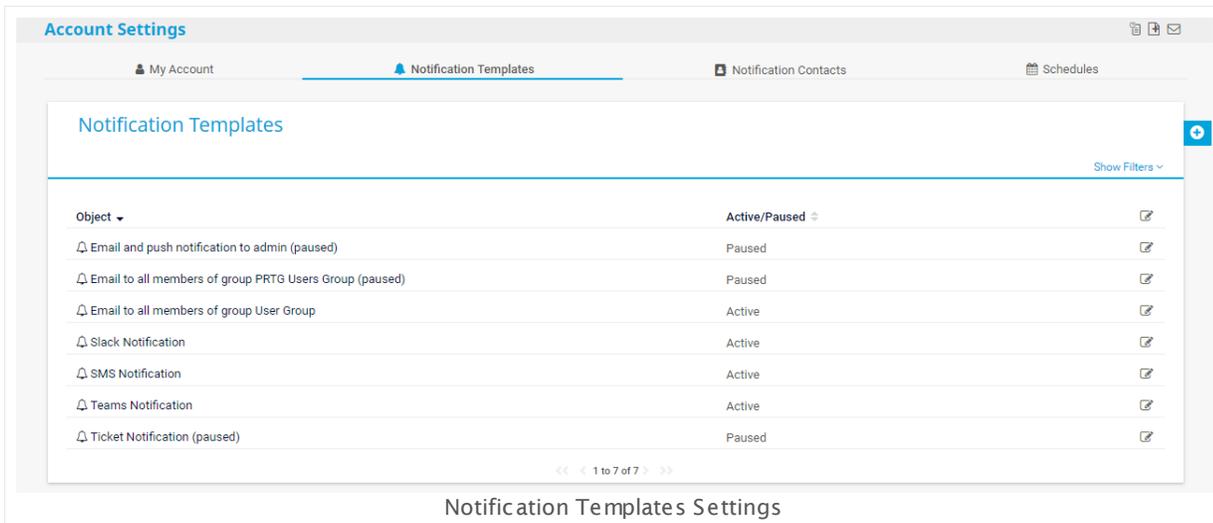
Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <https://kb.paessler.com/en/topic/26303>

8.12.2 Account Settings—Notification Templates

In the notification templates settings, you can define and change notifications for the current PRTG user. Notifications can be triggered for specific sensor states and values.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



Note

This section describes one of four steps to set up the notification system in PRTG. To complete your notification setup, go through all of the following steps:

1. Check and set up the **Notification Delivery** settings to define how and to which recipient PRTG will send messages.
For detailed information, see [System Administration—Notification Delivery](#) ³³⁶¹.
2. Check and set up **Notification Contacts** for the PRTG users to define the recipients of notifications.
For detailed information, see [Account Settings—Notification Contacts](#) ³³³⁴.
3. Check and set up **Notification Templates** to define the notification methods and their content.
For detailed information, see [Account Settings—Notification Templates](#) ³³¹¹.
4. Check and set up **Notification Triggers** for objects to define when notification messages will be sent.
For detailed information, see [Sensor Notification Triggers Settings](#) ³¹⁷⁰.

i We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one [email notification](#)^[3317] and one [SMS notification](#)^[3320]. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a [state trigger](#)^[3172] and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

 For background information, see the [Notifications](#)^[3216] section.

Notification Templates

Click the **Notification Templates** tab to show a list of existing notification templates. Using the **Edit** buttons on the right, perform the following actions to set up a notification template:

- **Send test notification:** Trigger this notification immediately for testing purposes.
 - i** When testing notifications, PRTG will not resolve the placeholders, but rather send the original variables instead.
- **Used by:** Show all objects that trigger this notification.
- **Pause:** Pause this notification. If a notification is [paused](#)^[245], PRTG will not send messages when this notification is triggered.
- **Resume:** Resume monitoring of a paused object at any time.
- **Delete:** Delete this notification (not possible for predefined notifications).
- **Settings:** Open the [settings of a notification template](#)^[3312].

Please also see [Working with Table Lists](#)^[237]. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the [Multi-Edit Lists](#)^[3197] section.

Notification Template Settings

Hover over  and select **Add Notification Template** from the menu to add a new notification template, or click the name of an existing notification template to edit it.

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

BASIC SETTINGS

Template Name	Enter a meaningful name for the notification template, for example, SMS to service team.
---------------	---

BASIC SETTINGS

Tags	Enter one or more tags ¹³⁹ . Confirm each tag with the space, comma, or enter key. You can use tags to group sensors and use tag-filtered views later on. Tags are not case sensitive. Tags will be automatically inherited ¹³⁹ .
Status	Select the status of the notification. Choose between: <ul style="list-style-type: none">▪ Started: This notification is active. PRTG executes this notification when it is triggered.▪ Paused: Pause this notification. If a notification is paused, PRTG does not execute this notification when it is triggered.
Schedule	Define intervals for notifications to pause. You might want the notifications to pause for scheduled maintenance periods or regular server reboots at certain intervals. For continuous notification select None . This selection will make your notifications be active 24/7 without pause. You can also choose one of the suggested schedules from the list. Usually schedules define when this notification will be active. Schedules defined as period list set this notification to inactive at the corresponding time spans. The available options depend on your setup.  To add or change existing schedules, see Account Settings—Schedules ³³⁸ .
Postpone	Define whether PRTG should send you notifications that were triggered while the notification was Paused later on, when the notification status is in Started again. <ul style="list-style-type: none">▪ No: Discard all notifications that are triggered while the notification is paused.▪ Yes: Collect all notifications that are triggered while the notification is paused. Send out all these notifications once the Paused status ends.

NOTIFICATION SUMMARIZATION

Method

Define if and how PRTG summarizes several notifications into one or more messages (max. 1,000 characters). Define if several notification triggers are to be collected over a specified time period and then send as a single summarized notification. Choose between:

- **Always notify ASAP, never summarize:** Always send out one notification for each received notification trigger as soon as possible (for example, immediately).
- **Send first DOWN message ASAP, then summarize:** When receiving several **DOWN** triggers, send the first notification immediately, then keep summarizing notification triggers into one message, regardless of sensor state.
- **Send first DOWN and UP message ASAP, then summarize:** When receiving several **DOWN** or **UP** triggers, send each first notification immediately, then keep summarizing notification triggers into one message, regardless of sensor state.
- **Send all DOWN messages ASAP, summarize the others:** When receiving several **DOWN** triggers, send out one notification for each trigger received, but summarize notifications for all non-**DOWN** triggers into one message.
- **Send all DOWN and UP messages ASAP, summarize the others:** When receiving several **DOWN** or **UP** triggers, send out one notification for each trigger received, but summarize the notifications for all non-**DOWN** and non-**UP** triggers into one message.
- **Always summarize notifications, regardless of type:** When receiving several notification triggers, summarize notifications, regardless of the kind of trigger received. Please note, the maximum number of notifications (see below) still applies.

 Regardless of the option you choose, PRTG never summarizes notifications of the types **Send Slack Message**, **Send Microsoft Teams Message**, **Execute HTTP Action**, **Execute Program**, and **Assign Ticket** because it always sends them immediately. The messages of all other notification types can be summarized.

 'first DOWN' and 'first UP' messages refer to trigger condition and clear condition respectively. You can also define 'WARNING' or 'UNUSUAL' states as trigger conditions or even thresholds or other triggers notification summarizations. The condition clear triggers, if applicable, are defined in the respective trigger conditions as well. The triggers all qualify as "first DOWN" or "first UP" messages.

NOTIFICATION SUMMARIZATION

 PRTG collects up to 25 single notifications for one summarization and will send out the message as soon as this number is reached (or when the gathering time has passed). If there are more than 25 notifications within the defined time span, you will receive more than one message with up to 25 entries each. For example, 74 collected notifications would result in 3 summarized messages with 25, 25, and 24 collected notifications.

Subject for Summarized Messages

Define a subject that PRTG will include when sending summarized notifications. You can use the placeholder **%SUMMARYCOUNT** for the number of messages that are summarized.

 The subject you define is only used for **Send Email** and **Amazon SNS** messages.

Timespan for Summarizing Messages (in Minutes)

Define a time span in minutes to define how long PRTG collects notifications for summarization. Please enter an integer value.

 If you enter a rather long time span, for example, **60** minutes, PRTG will collect notifications for one hour before sending them out summarized unless other features (see above) require an earlier message dispatch.

ACCESS RIGHTS

User Group Access Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
- **Read:** Users in this group can see the object and review its settings.
- **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the [System Administration—User Groups](#) settings.

Notification Templates Settings—Choose Notification Methods

With the following settings, you can add one or more methods for how PRTG sends out a notification message. You can choose one method or combine several methods from the list. Whenever the notification is triggered, PRTG sends out messages or performs actions for all configured methods at once.

To choose a method, mark the check box in front of the corresponding notification type. You can then see and set the options as described below. The following notification methods are available.

- [Email](#)
- [Push Notification](#)
- [SMS/Pager Message](#)
- [Slack Message](#)
- [Microsoft Teams Message](#)
- [Add Entry to Event Log](#)
- [Syslog Message](#)
- [SNMP Trap Message](#)
- [Execute HTTP Action](#)
- [Execute Program](#)

- [Amazon SNS Message](#) 
- [Ticket](#) 

 In your message, you can use various placeholders. Some of them are already filled in by default. For a complete list of available placeholders, see this Knowledge Base article: [What placeholders can I use with PRTG?](#)

- Some notification types are only available for PRTG on premises (marked with the PRTG on premises icon). You cannot use these on PRTG hosted by Paessler instances.

SEND EMAIL

 This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under [Account Settings — Notification Contacts](#) .

 The three options for recipients below (user, user group, email address) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification email to the active email contacts of the user you select, to the active email contacts of all members of the user group you select, and to all email addresses you enter into the **Send to Email Address** field.

 You can include custom email headers and footers into PRTG HTML emails. For details, see this Knowledge Base article [How can I include my own logo into HTML emails?](#)

Sender	Define which email address and sender name will appear in the FROM part of your email notifications. Choose between: <ul style="list-style-type: none"> ▪ Default: Use the default sender email and name as defined in the global Notification Delivery  settings. ▪ Custom: Override the global sender email and name.
Sender Email Address	Enter an email address to use as sender of all email notifications. This field overrides the global setting from the Notification Delivery  tab. The default value is the global sender email. <p> The email address must be allowed by the outgoing SMTP server defined in the Notification Delivery  settings.</p>
Sender Name	Enter a sender to use as sender of all email notifications. This field overrides the global setting from the Notification Delivery  tab. The default value is the global sender name.

SEND EMAIL

- Send to User** Select a user of your PRTG installation to send the notification email to. PRTG sends this notification to each email contact of this user account. You can add and edit email contacts of a user in [Account Settings—Notification Contacts](#)³³³⁵. Choose **None** to not use this feature.
- Send to User Group** Select a user group to send an email with the notification to all members of this group. PRTG sends this notification to the email contact of every group member. You can edit user groups under [System Administration—User Groups](#)³³³⁵ and email contacts under [Account Settings—Notification Contacts](#)³³³⁵. Choose **None** to not use this feature.
- ❗ If you select a user group and a specific member of this group as recipients, the user will only receive a single email. This also applies if you enter an individual email address below that is already defined as an email contact of the selected user.
 - ❗ If you define individual email addresses (see below), to a specific user (see above), and a user group, PRTG sends the message to the individual email addresses, to the individual user, as well as to the members of the selected user group. In all cases, PRTG sends one message with all recipients in the "To" field of the email.
- Send to Email Address** Enter one or more recipient email addresses to which PRTG sends the notification email. If you enter more than one address, separate them with commas. Leave this field empty to send this notification only to the email contacts of the user or members of the user group you choose above.
- We recommend that you use the options **Send to User** and/or **Send to User Group** instead because you can manage the notification contacts of users more easily this way.
- Subject** Enter the subject of the email notification.
- Several [placeholders](#)³³³² (variables) are used here by default: [%
sitename] %device %name %status %down (%message)
- Format** Define the kind of email that PRTG sends when the notification is triggered. Choose between:
- **HTML:** PRTG uses the default HTML email template for the message part of the email.
 - ❗ Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG.

SEND EMAIL

- **Text**: PRTG uses the default plain text email template for the message part of the email.
- **Text with custom content**: PRTG uses custom plain text for the message part of the email. You can enter your individual text below.

Custom Content This field is only visible if you select the custom text option above. Enter the desired message for this email notification in plain text format. You can use [placeholders](#) ^[3332] here.

Priority Define the priority that PRTG sets for the email. Most email clients can show this priority flag. Choose between:

- **highest**
- **high**
- **normal**
- **low**
- **lowest**

SEND PUSH NOTIFICATION

 Push notifications only work with the apps [PRTG for Android](#) ^[3485] and [PRTG for iOS](#) ^[3484]. You have to activate push notifications in the settings of your app first. For details about the setup, see this Knowledge Base article: [How can I send push notifications with PRTG?](#)

 This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under [Account Settings —Notification Contacts](#) ^[3335].

 The PRTG server needs to communicate on port 443 to the PRTG Cloud to send push notifications, which is <https://api.prtgcloud.com:443> (the same as for the [Cloud HTTP Sensor](#) ^[619], the [Cloud Ping Sensor](#) ^[629] and [support tickets](#) ^[3424]).

 The two options for recipients below (user, user group) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification to the active push contacts of the user you select and to the active push contacts of all members of the user group you select.

SEND PUSH NOTIFICATION

- Send to a User** Select a user of your PRTG installation to send the push notification to. PRTG sends this notification to each push contact of this user account. You can edit push contacts of a user in [Account Settings—Notification Contacts](#)³³³⁵ and add push contacts by activating push notifications in the Android or iOS app with this user. Choose **None** to not use this feature.
- Send to a User Group** Select a user group to send the push notification to all members of this group. PRTG sends this notification to each push contact of every member of this group. You can edit user groups under [System Administration—User Groups](#)³³⁸³ and push contacts under [Account Settings—Notification Contacts](#)³³³⁵. Choose **None** to not use this feature.
-  If you select a user group and a specific member of this group as recipients at the same time, this user receives the text message only one time.
- Message** Define the message. A message with information about the sensor status is already predefined. Several [placeholders](#)³³³² (variables) are used here: [%sitename] %device %name %status %down (%message)
- You can change the message to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

SEND SMS/PAGER MESSAGE

-  You have to set up this notification method in the [System Administration—Notification Delivery](#)³³⁶¹ settings first.
-  This notification method uses notification contacts to deliver the messages. Please set up and check them for the desired user accounts in advance under [Account Settings—Notification Contacts](#)³³³⁵.
-  The three options for recipients below (user, user group, email address) work simultaneously. Because of this, you can define more than one user as recipient of this notification. PRTG sends the notification to the active SMS contacts of the user you select, to the active SMS contacts of all members of the user group you select, and to every phone number you enter into the **Send to Number** field.
-  This notification method uses the central proxy settings that you define for your PRTG core server. For details, see [System Administration—Core & Probes](#)³³⁶⁸ (section **Proxy Configuration**).

SEND SMS/PAGER MESSAGE

Send to User	<p>Select a user of your PRTG installation to send the notification to. PRTG sends this notification to each SMS contact of this user account. You can add and edit SMS contacts of a user in Account Settings—Notification Contacts^[3335]. Choose None to not use this feature.</p>
Send to User Group	<p>Select a user group to send a text message with the notification to all members of this group. PRTG sends this notification to each SMS contact of every member of this group. You can edit user groups under System Administration—User Groups^[3383] and SMS contacts under Account Settings—Notification Contacts^[3335]. Choose None to not use this feature.</p> <p>i If you select a user group and a specific member of this group as recipients at the same time, this user receives the text message only one time. This also counts if you enter an individual phone number below that is already defined as an SMS contact of the selected user.</p>
Send to Number	<p>Define the number to which PRTG sends the text message. The format depends on the SMS provider. Usually, you use a plus sign "+", followed by country code and number. For example, enter +1555012345.</p> <p>i Ensure the number format meets the requirements of your SMS provider or the hardware that you use in combination with an API call. Sometimes a preceded plus sign is not required. A wrong format may result in undelivered messages!</p> <p>If you enter more than one number, separate them by comma. Leave this field empty to send this notification only to the SMS contacts of the user or members of the user group you choose above.</p> <p>We recommend that you use the options Send to User and/or Send to User Group instead because you can manage the notification contacts of users more easily this way.</p>
Message	<p>Define the message. A message with information about the sensor status is already predefined. Several placeholders^[3332] (variables) are used here: [%sitename] %device %name %status %down (%message)</p> <p>You can change the message to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).</p>

SEND SLACK MESSAGE

 Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Send Slack Message** always as soon as possible (ASAP). They are never summarized.

URL of Slack Webhook	Enter the URL of the incoming webhook that you set up in your Slack workspace.
Sender Name	Enter a sender name to use as sender of Slack notifications. This field overrides the sender that you may have defined in your Slack workspace.
Title	Enter the title of your Slack notification. The following placeholders  (variables) are used here by default: %device %name
Subtitle	Enter the subtitle of your Slack notification. The following placeholder  (variable) is used here: %message
Content	Choose between the following options to define the content of your Slack notification: <ul style="list-style-type: none">▪ Use default content: The notification message will include information about the Status, Last Scan, Last Value, Last Up, Coverage, Downtime, Priority, Probe, and Group.▪ Define custom content: The notification message will include the pieces of information that you choose in the Content options (see next step).
Select Content	This field is only visible if you select the Define custom content option above. Add a check mark in front of the piece of monitoring information that you want PRTG to include in your Slack notification. Remove the check mark in front of the items that you do not want to include. Multiple choices are possible. The following types of monitoring information are available: <ul style="list-style-type: none">▪ Name▪ Host▪ Status▪ Last Scan▪ Last Value

SEND SLACK MESSAGE

- **Message**
- **Last Down**
- **Last Up**
- **Coverage**
- **Downtime**
- **Uptime**
- **Priority**
- **Probe**
- **Group**
- **Device**
- **Date and time**
- **Timezone**
- **Comments (probe)**
- **Comments (group)**
- **Comments (device)**
- **Comments (sensor)**
- **History**

For more information on these types of monitoring information, please refer to the [placeholders](#)³³³².

SEND MICROSOFT TEAMS MESSAGE

 Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Send Microsoft Teams Message** always as soon as possible (ASAP). They are never summarized.

URL of Teams Webhook Enter the URL of the incoming webhook that you set up in your Microsoft Teams workspace.

Title Enter the title of your Microsoft Teams notification.

The following [placeholders](#)³³³² (variables) are used here by default:
%device %name

SEND MICROSOFT TEAMS MESSAGE

Subtitle	<p>Enter the subtitle of your Microsoft Teams notification.</p> <p>The following placeholder³³³² (variable) is used here: %message</p>
Content	<p>Choose between the following options to define the content of your Microsoft Teams notification:</p> <ul style="list-style-type: none">▪ Use default content: The notification message will include information about the Status, Last Scan, Last Value, Last Up, Coverage, Downtime, Priority, Probe, and Group.▪ Define custom content: The notification message will include the pieces of information that you choose in the Content options (see next step).
Select Content	<p>This field is only visible if you select the Define custom content option above.</p> <p>Add a check mark in front of the piece of monitoring information that you want PRTG to include in your Microsoft Teams notification. Remove the check mark in front of the items that you do not want to include.</p> <p>Multiple choices are possible.</p> <p>The following types of monitoring information are available:</p> <ul style="list-style-type: none">▪ Name▪ Host▪ Status▪ Last Scan▪ Last Value▪ Message▪ Last Down▪ Last Up▪ Coverage▪ Downtime▪ Uptime▪ Priority▪ Probe▪ Group▪ Device

SEND MICROSOFT TEAMS MESSAGE

- **Date and time**
- **Timezone**
- **Comments (probe)**
- **Comments (group)**
- **Comments (device)**
- **Comments (sensor)**
- **History**

For more information on these types of monitoring information, please refer to the [placeholders](#) [3332].

ADD ENTRY TO EVENT LOG

 This option is not available in PRTG hosted by Paessler.

Logfile	<p>Define the logfile into which PRTG writes the message. Choose between:</p> <ul style="list-style-type: none"> ▪ Application: Use the Windows application logfile in the event log. ▪ PRTG Network Monitor: Write messages to the PRTG Network Monitor logfile in the Windows event log.
Event Source	<p>This setting is only relevant when using the Application logfile. Enter the source for the event. Usually, this is the name of the application.</p>
Event Type	<p>Select the type of the event. Choose between:</p> <ul style="list-style-type: none"> ▪ Error ▪ Warning ▪ Information
Event Log Message	<p>Define the message. A message with information about the sensor status is already predefined. Several placeholders [3332] (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).</p>

SEND SYSLOG MESSAGE

 This option is not available in PRTG hosted by Paessler.

Host/IP	Define the IP address or DNS name of the computer running the syslog server.  You can receive and analyze syslog messages with the Syslog Receiver Sensor ²⁶⁵⁹ .
Syslog Port	Enter the port number on which syslog messages are sent. By default, this is port number 514.  Only User Datagram Protocol (UDP) is supported.
Facility	Define the facility information. There are several options available from the list.
Encoding	Define the encoding of the syslog message that PRTG sends to your syslog receiver. Choose between: <ul style="list-style-type: none"> ▪ ANSI ▪ UTF-8
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders ³³²⁶ (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).

SEND SYSLOG MESSAGE—SYSLOG MESSAGE SEVERITY STATUS

 Depending on the status of the sensor that triggers the syslog notification, PRTG sets the **Severity** level of the message automatically.

 OK	Severity level: Notice (5)
 Warning	Severity level: Warning (4)
 Error	Severity level: Error (3)

SEND SNMP TRAP



For information about the OIDs that PRTG uses in the content of the SNMP traps, see this Knowledge Base article: [Is it possible to send SNMP traps using PRTG?](#)



This option is not available in PRTG hosted by Paessler.

Host/IP	Define the IP address or DNS name of the computer running the trap receiver.  You can receive and analyze SNMP trap messages with the SNMP Trap Receiver Sensor <small>2479</small> .
SNMP Port	Enter the port number on which trap messages are sent. By default, this is port number 162 .
Community String	Enter the community string of the device. By default, this is set to public . Please enter a string or leave the field empty.
Specific Trap Code	Enter a code that can help you identify the purpose of the trap. Default value is 0 . Please enter an integer value.
Message ID	Enter an ID that helps you identify the origin of the trap. Please enter an integer value. PRTG sends it on the OID 1.3.6.1.4.1.32446.1.1.1 .
Message	Define the message. A message with information about the sensor status is already predefined. Several placeholders <small>3332</small> (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).
Agent IP	Define the IP address of the agent. Leave this field empty to use the IP address of your PRTG web server.

EXECUTE HTTP ACTION



Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Execute HTTP Action** always as soon as possible (ASAP). They are never summarized.

EXECUTE HTTP ACTION

 This notification method uses the central proxy settings that you define for your PRTG core server. For details, see [System Administration—Core & Probes](#)³³⁰⁸ (section **Proxy Configuration**).

 For more details, see section [Custom Notifications](#)³³⁰⁹. You can find ready-to-use custom notifications in the PRTG Script World, see [below](#)³³³¹.

URL	<p>Enter the URL to which PRTG sends the request.</p> <p> HTTP notifications work with and without SSL.</p>
SNI (Server Name Indication)	<p>Select if PRTG will send the SNI extension to the TLS protocol along with the HTTP request. Choose between:</p> <ul style="list-style-type: none"> ▪ Do not send SNI (default): PRTG will not send an SNI when executing the HTTP action. ▪ Send SNI: PRTG will send an SNI when calling the target URL. Specify the SNI below.
Virtual Host (SNI)	<p>This field is only visible if you select the SNI option above. Enter the SNI name that your endpoint configuration requires. Usually, this is the Fully Qualified Domain Name (FQDN) of the virtual host.</p>
HTTP Method	<p>Choose the HTTP method that you want PRTG to use. Choose between:</p> <ul style="list-style-type: none"> ▪ GET ▪ POST ▪ PUT ▪ PATCH
Payload	<p>This field is only visible if you choose POST, PUT, or PATCH above.</p> <p>Enter a payload here. The payload is the data that PRTG will transmit to the URL you have specified. You can use placeholders³³³² here. Line breaks are supported.</p>

EXECUTE PROGRAM

 Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Execute Program** always as soon as possible (ASAP). They are never summarized.

 For more details, see section [Custom Notifications](#)³⁶⁵⁸. You can find ready-to-use custom notifications in the PRTG Script World, see [below](#)³³³¹.

 This option is not available in PRTG hosted by Paessler.

Program File Select an executable file from the list. PRTG runs it every time the notification is triggered. In this list, you see the files that are in the corresponding **/Notifications/EXE** sub-directory of your PRTG core server system. To appear in this list, store the files as BAT, CMD, DLL, EXE, PS1, or VBS.

 To find this path, see section [Data Storage](#)³⁷³⁴.

 In a cluster setup, copy your files to every cluster node installation manually. This makes sure PRTG can execute the notification even when the master node fails. If your custom notification executes an external program, install it on all cluster nodes as well.

Parameters Enter parameters with which the program file will be started. You can use [placeholders](#)³³³² here. For example, if you use a batch file that contains a **%1** variable, you can provide a value for this variable here.

 You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section [Escape Special Characters and Whitespaces in Parameters](#)³³¹¹ for details.

Domain or Computer Name Enter a Windows authority if you want to use another security context for the program than the security context of the PRTG probe service.

Username Enter the username for Windows access.

Password Enter the password for Windows access.

Timeout Enter a timeout in seconds. After this time has passed, PRTG stops the process if it has not terminated yet. Please enter an integer value.

SEND AMAZON SIMPLE NOTIFICATION SERVICE MESSAGE

AWS Access Key ID	Enter your access key as shown in your login area at aws.amazon.com. Please enter a string.
AWS Secret Access Key	Enter your secret access key as shown in your login area at aws.amazon.com. Please enter a string.
Location	<p>Define the location of your Amazon service. Choose one of the shown locations:</p> <ul style="list-style-type: none">▪ US East (Northern Virginia)▪ US West (Ohio)▪ US West (Northern California)▪ US West (Oregon)▪ Canada (Central)▪ EU West (Ireland)▪ EU Central (Frankfurt)▪ EU (London)▪ Asia Pacific (Singapore)▪ Asia Pacific (Sydney)▪ Asia Pacific (Seoul)▪ Asia Pacific (Tokyo)▪ Asia Pacific (Mumbai)▪ South America (Sao Paulo)
ARN	Enter the Amazon resource name. Please enter a string.
Subject	<p>Enter the subject of the message. Please enter a string.</p> <p> The maximum length for the subject is 202 characters. Characters that exceed this number will be cut off.</p>
Message	<p>Define the message. A message with information about the sensor status is already predefined. Several placeholders³³³² (variables) are used here. You can change it to your liking. To reset this field to its default value, enter a single star symbol * (and nothing else).</p> <p> The message part is only sent if you use email based notifications delivered by Amazon SNS. For SMS delivery, only the subject is sent while the message part is ignored because of SMS size restrictions.</p>

ASSIGN TICKET

 Regardless of the **Notification Summarization** method chosen above, PRTG sends notifications of the type **Assign Ticket** always as soon as possible (ASAP). They are never summarized.

 For details about the ticket system, see manual section [Tickets](#)²³⁰.

Assign to User or User Group Specify whether to assign the notification ticket to a user group or to a single user. Choose between:

- **To User Group:** Select a user group below to which PRTG assigns this ticket.
- **To User:** Select the dedicated user below to whom PRTG assigns this ticket.

Assign Ticket to this User Group / User Select the user or user group to which PRTG assigns the notification ticket.

Subject Enter the subject of the ticket. Several placeholders (variables) are used here by default. You can change it to your liking.

Content Define the message in the ticket. A message with information about the sensor status is already predefined. Several [placeholders](#)³³³² (variables) are used here. You may change it as you wish.

When Condition Clears Specify if PRTG closes the ticket automatically when the defined trigger condition clears. Choose between:

- **Close ticket automatically (recommended):** PRTG closes the ticket automatically if the trigger condition is not met anymore.
- **Leave ticket open:** PRTG does not close the ticket after the condition has cleared.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Script World Notifications

In addition to the built-in notification, you can create your own notifications. Just write a script or a program and use it with an **Execute Program** notification or execute an HTTP action. There are already many free, useful scripts, plugins, and add-ons for PRTG in the [PRTG Script World](#) available for download. Here is a list of the custom notifications that you can find there.

- How to Send Custom HTML Notifications

- Sending Notifications Using Telegram Bots

Others

 For information about the comments and history tabs, see [Object Settings](#)²¹⁷ section.

Escape Special Characters and Whitespaces in Parameters

 You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ":", "_", "-", "=", and "/" outside of quoted strings.

 We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#)³⁶⁵ for details.

More

- [Custom Notifications](#)³⁶⁶
- [Setting up Notifications Based on Sensor Limits: Example](#)³²¹⁹
- [Setting up Notifications Based on Libraries: Example](#)³²²⁹

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

Knowledge Base: Documentation of SNMP Traps Sent by PRTG

- <https://kb.paessler.com/en/topic/1133>

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- <https://kb.paessler.com/en/topic/14803>

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <https://kb.paessler.com/en/topic/26303>

Knowledge Base: How can I send push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

How can I include my own logo into HTML emails?

- <https://kb.paessler.com/en/topic/65782>

8.12.3 Account Settings—Notification Contacts

In the **Notification Contacts** settings the PRTG user who is currently logged in defines and changes their notification contacts.

Notification contacts are unique for each user account. That is, every user of a PRTG installation can individually define how they want to get notified by PRTG. Recipients of [notifications](#)^[3216] are email addresses, phone numbers, push devices (with [PRTG for Android](#)^[3485] or [PRTG for iOS](#)^[3484]), and users of certain instant messaging services.

The [notification methods](#)^[3316] **Send Email**, **Send SMS/Pager Message**, or **Send Push Notification** allow you to set a PRTG user who will receive notifications at **all** their **active** notification contacts. If you select a user group, PRTG will send the notifications to **all active** contacts of **all** users that are in this group. To exclude defined notification contacts from notification delivery, you can use the **pause** feature to deactivate them.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Note

This section describes one of four steps to set up the notification system in PRTG. To complete your notification setup, go through all of the following steps:

1. Check and set up the **Notification Delivery** settings to define how and to which recipient PRTG will send messages.
For detailed information, see [System Administration—Notification Delivery](#)^[3361].
2. Check and set up **Notification Contacts** for the PRTG users to define the recipients of notifications.
For detailed information, see [Account Settings—Notification Contacts](#)^[3334].
3. Check and set up **Notification Templates** to define the notification methods and their content.
For detailed information, see [Account Settings—Notification Templates](#)^[3311].
4. Check and set up **Notification Triggers** for objects to define when notification messages will be sent.
For detailed information, see [Sensor Notification Triggers Settings](#)^[3170].

ⓘ We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one [email notification](#)^[3317] and one [SMS notification](#)^[3320]. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a [state trigger](#)^[3172] and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

■ For background information, see the [Notifications](#)^[3216] section.

Notification Contacts Overview

Click on the **Notification Contacts** tab to show a list of all existing notification contacts of the currently logged in PRTG user. Using the buttons in the particular contact rows, you can do the following:

- **Pause:** Pause this notification contact. If a notification contact is [paused](#)²⁴⁵, PRTG does not send any messages to this contact when a notification for this user is triggered.
- **Edit:** Open the [settings of this notification contact](#)³³⁵ and change its description and recipient.
 - ❗ This is not possible for predefined notification contacts, for example, the primary email address. You can change the primary email address under [Account Settings—My Account](#)³³⁴.
- **Delete:** Delete this notification contact.
 - ❗ This is not possible for predefined notification contacts, for example, the primary email address.

Notification Contacts Settings

Hover over  and select **Add Email Contact** or **Add SMS Contact** to add a new notification contact, or click the **Edit** button of an existing notification contact to edit it. A dialog box appears where you can enter the contact settings.

❗ PRTG adds push contacts automatically for the corresponding user when you install a PRTG mobile app on your smartphone or tablet, connect to the PRTG server, and activate push notifications. You cannot add push contacts manually. If your mobile device rejects push notifications actively for an existing push contact, for example, because you deactivated push on the target device or reset it, the PRTG server will [pause](#) this contact automatically. The affected PRTG user account will receive a [ToDo ticket](#)²³⁰ in this case.

ADD NEW / EDIT NOTIFICATION CONTACT

Description	Enter a meaningful name for the notification contact, for example, SMS to Admin Mobile or similar.
Recipient	<p>Enter a valid email address for the contact type Email. You can add an SMS contact by entering a valid phone number. The format of the phone number depends on the SMS provider. Usually, you use a plus sign "+", followed by country code and number. For example, enter +1555012345</p> <p>❗ Ensure the number format meets the requirements of your SMS provider or the hardware that you use in combination with an API call. Sometimes a preceded plus sign is not required. A wrong format may result in undelivered messages!</p>

ADD NEW / EDIT NOTIFICATION CONTACT

 For the contact type **Push**, this field shows a unique token that you cannot change here. This token is needed to send push notifications through the cloud. For details, see this Knowledge Base article: [How can I use push notifications with PRTG?](#)

Contact Type Shows the type of contact, either **Email**, **SMS**, or **Push**. This setting is shown for your information only and cannot be changed here.

If you want to use another contact type, create a new contact with **Add Email Contact** or **Add SMS Contact**, or activate push notifications in your PRTG for iOS or Android app.

Click the **Save** or **Add** button to save your settings, or click **Cancel** to close the dialog box without changes to your configuration.

A cloud contact is added automatically when you install the PRTG app on your smartphone, connect to the PRTG server, and enable push notifications.

More

Knowledge Base: How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

Setup—Topics

- [Account Settings—My Account](#)  3304
- [Account Settings—Notification Templates](#)  3311
- [Account Settings—Notification Contacts](#)  3334
- [Account Settings—Schedules](#)  3338
- [System Administration—User Interface](#)  3343
- [System Administration—Monitoring](#)  3355
- [System Administration—Notification Delivery](#)  3361
- [System Administration—Core & Probes](#)  3368
- [System Administration—User Accounts](#)  3376
- [System Administration—User Groups](#)  3383
- [System Administration—Cluster](#)  3394
- [System Administration—Administrative Tools](#)  3388
- [PRTG Status—System Status](#)  3396
- [PRTG Status—Auto-Update](#)  3407
- [PRTG Status—Cluster Status](#)  3412
- [PRTG Status—Activation Status](#)  3414
- [Downloads and Tools](#)  3420
- [Desktop Notifications](#)  3422
- [Support—Contact Support](#)  3424

Others

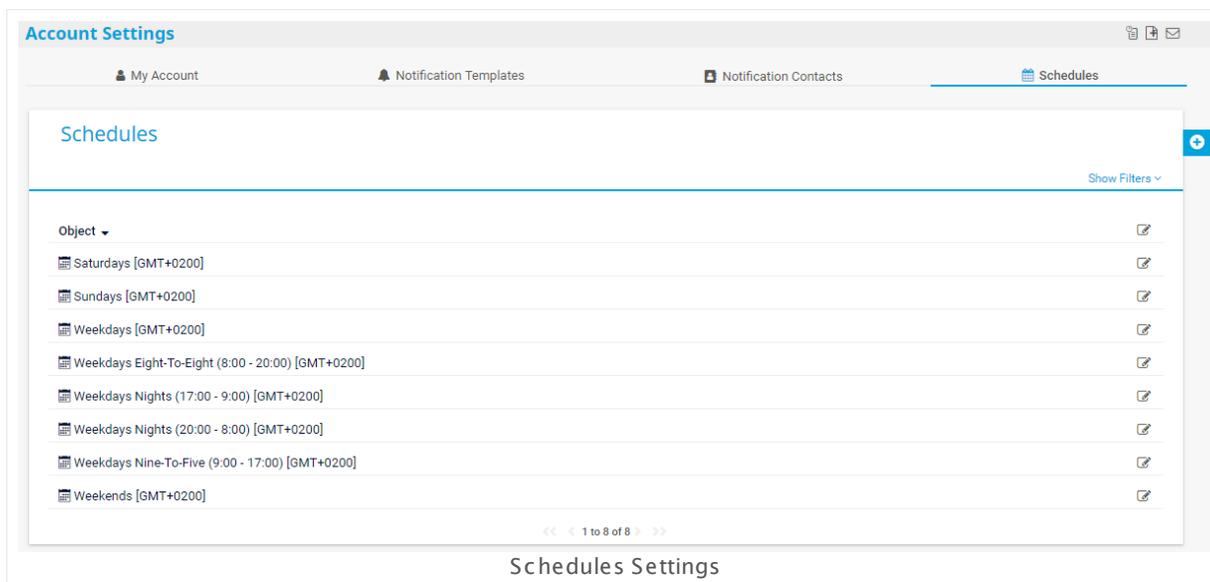
There are some settings that you must make in the [PRTG Administration Tool](#)  3560, available as native Windows application. For more details, see the sections:

- [PRTG Administration Tool on Core Server System](#)  3561
- [PRTG Administration Tool on Remote Probe System](#)  3567

8.12.4 Account Settings—Schedules

In the schedule settings you can define or change schedules for the currently logged in user. You can use schedules to [pause](#)^[245] monitoring/notification at for certain time periods with the period lists option. Also you can activate it at certain times with the time table option. You can also use schedules to define the time periods that are to be covered when creating [reports](#)^[325].

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.



Schedules Settings

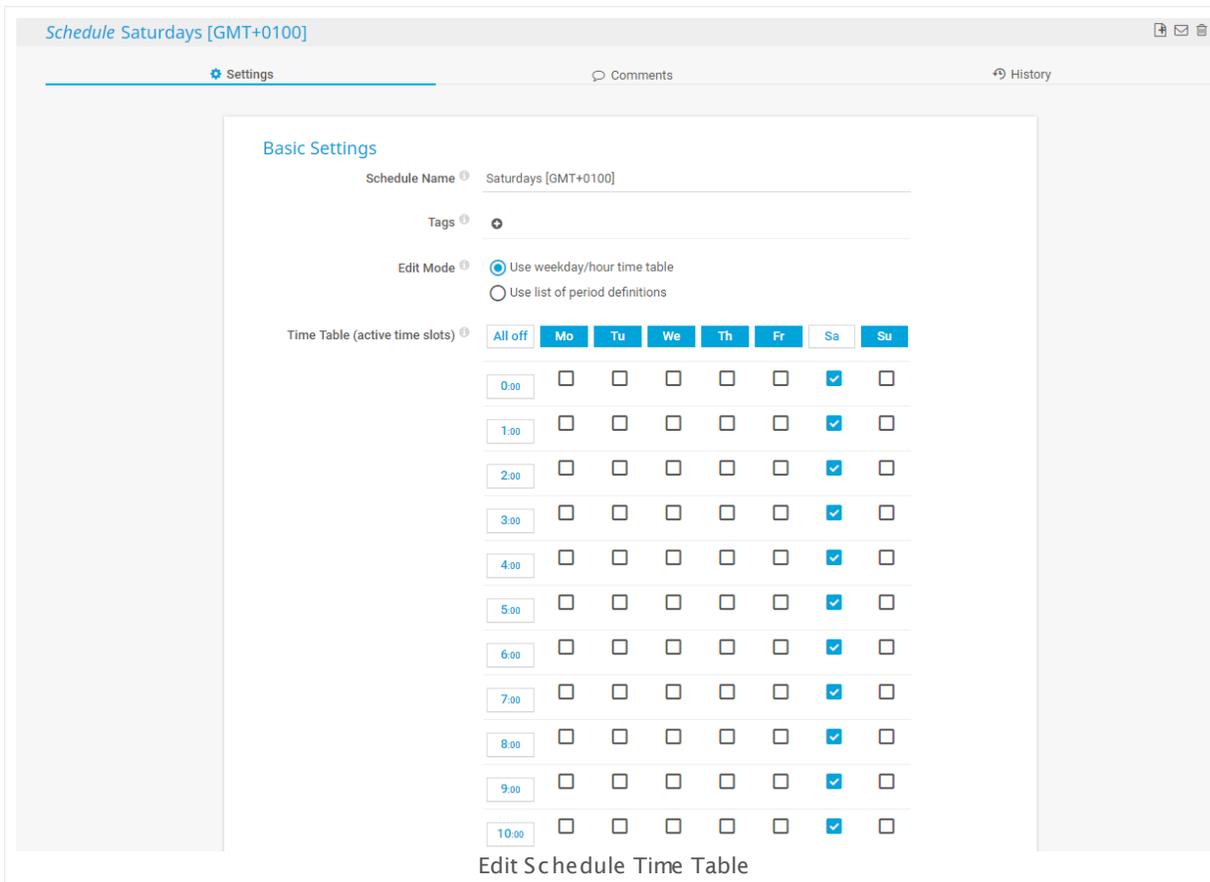
i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Click on the **Schedules** tab to show a list of all existing schedules. Using the **Edit** button, you can perform the following actions:

- **Used by:** Show a list of objects using this notification.
- **Delete:** Delete this notification (not possible for predefined notifications)
- **Settings:** Shows the settings of the selected schedule.

Please also see [Working with Table Lists](#)^[237]. Additionally, the multi-edit functionality is available. This enables you to change properties of several objects simultaneously via bulk changes. For more details, see the [Multi-Edit Lists](#)^[319] section.

Hover over  and select **Add Schedule** or click the name of an existing notification to edit.



BASIC SETTINGS

Schedule Name Enter a meaningful name for the schedule that describes the defined time span(s) or their purpose.

Tags Use tags to filter for objects of certain categories. See section [Tags](#) ¹³⁹ for more information.

Edit Mode Select how you want to define a schedule. Choose between:

- **Use weekday/hour time table:** Define a schedule by adding check marks to available check boxes. The lowest possible increment is one hour.
 -  This time table defines which time slots are **active**.

BASIC SETTINGS

- **Use list of period definitions:** Define a schedule by entering text lines using a specific syntax (see below).

 This time table defines which time slots are **inactive**.

Time Table

This selection is only visible if you enable the time table option above. Define the schedule. It will be used for monitoring objects, reporting, and notifications.

You can set time spans with a precision of one full hour by adding check marks. If a box is checked, it means the object is active during this hour. If unchecked, the object will be paused during this hour. You can set check marks individually, or change complete ranges for certain days of the week or time spans.

- To add ranges of check marks, use the weekday buttons **Mo**, **Tu**, **We**, **Th**, **Fr**, **Sa**, and **Su**, as well as the time buttons on the left side. If the color of a button is blue, a click will select the range. To select all ranges, click **All on**.
- To remove ranges of check marks, use weekday and time buttons that are active. If the color of a button is white, a click will deselect the range. To remove all ranges, click **All of**.

Period List

This field is only visible if you enable period definitions above. Define the date/time ranges in which the objects using this schedule will be **inactive** (for example, paused). During other times, the objects will be active. Enter the ranges in this format:

- **ww:hh:mm-ww:hh:mm**

 Ensure you enter each period exactly in the required syntax! Otherwise you will receive an error message. Please go back to the schedule and correct the according entry in this case.

 For details and examples, see [Schedules Settings—Period Definition Syntax](#)³³⁴¹ below.

 Schedules use the time zone of the computer on which your PRTG core server is running. This may diverge to other time displays in PRTG that are saved in UTC.

- If you define a schedule with the Time Table option in the [schedule settings](#)³³³⁹, the time to which the schedule applies is converted to the time zone of [your PRTG user account](#)³³⁰⁷. This means that the schedule is executed according to the time that your user account shows.
- If you use the Period List option, PRTG will **not** adjust the schedule to the time zone of your user account! The schedule will apply according to the time on your PRTG server in this case. Because of this, you will encounter time shifts for schedules if there are changes to the time zone on the server or in case of different daylight saving and standard time changes.

ACCESS RIGHTS

User Group Access Define which user group(s) will have access to the object that you are editing. A table with user groups and rights is shown; it contains all user groups from your setup. For each user group you can choose from the following access rights:

- **Inherited:** Use the settings of the parent object.
- **None:** Users in this group cannot see or edit the object. The object does not show up in lists.
- **Read:** Users in this group can see the object and review its settings.
- **Write:** Users in this group can see the object, as well as review and edit its settings. However, they cannot edit access rights settings.
- **Full:** Users in this group can see the object, as well as review and edit its settings as well as edit access rights.

You can create new user groups in the [System Administration—User Groups](#) settings.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Schedules Settings—Period Definition Syntax

Define one or more periods of time during which the object using this schedule will be **inactive**. In each line, enter one range in the format **ww:hh:mm-ww:hh:mm**: weekday, hour, minute.

- **Possible values for ww:** mo, tu, we, th, fr, sa, su.
- **Possible values for hh:** Enter the hour in 24 hour format (no AM/PM allowed), for example, a number between 00 and 23.
- **Possible values for mm:** Enter the minute, for example, a number between 00 and 59.

Example

This example shows a schedule that pauses an object during the weekend as well as on Wednesday evenings.

```
fr:19:30-mo:06:05
we:18:45-we:23:00
```

Any object using this schedule will be paused from Friday, 7:30 p.m. to Monday, 6:05 a.m. as well as on Wednesday from 6:45 p.m. to 11 p.m. It will be active during the other times.

Others

 For information about the comments and history tabs, see the [Object Settings](#)²¹⁷ section.

8.12.5 System Administration—User Interface

In the user interface settings you can define global values regarding the PRTG website appearance, PRTG web server settings and performance, Geo Maps, and graph settings.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

User Interface Settings

ⓘ This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

WEBSITE

PRTG Site Name When using the web interface, the site name is shown in the title bar of your browser window. It is also used by default in notification emails. Please enter a string.

DNS Name If your PRTG web interface is (additionally) reachable via a DNS name, enter it here. It is used, for example, by default in notification emails to generate links. Please enter a string.

ⓘ The special characters " and \ are not allowed in the DNS Name.

☁ This option is not available in PRTG hosted by Paessler.

Website Language Choose the system language from the dropdown list. Default is **English**. Depending on your installation, you may be able to choose other languages here. This setting defines the language of the [PRTG web interface](#)^[166], as well as of the [PRTG Administration Tool](#)^[3560].

ⓘ If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [PRTG Apps for Mobile Network Monitoring](#)^[3484] will be disconnected and reconnected.

WEBSITE

Graph Type Select how graphs will be displayed throughout the web interface and in [reports](#).

- **Use area graphs (recommended):** Display filled graphs.
- **Use line graphs:** Display graphs using single lines only.

We recommend using area charts, as they're better to read.

 Graphs containing data from more than one cluster node will always be displayed with line graphs automatically.

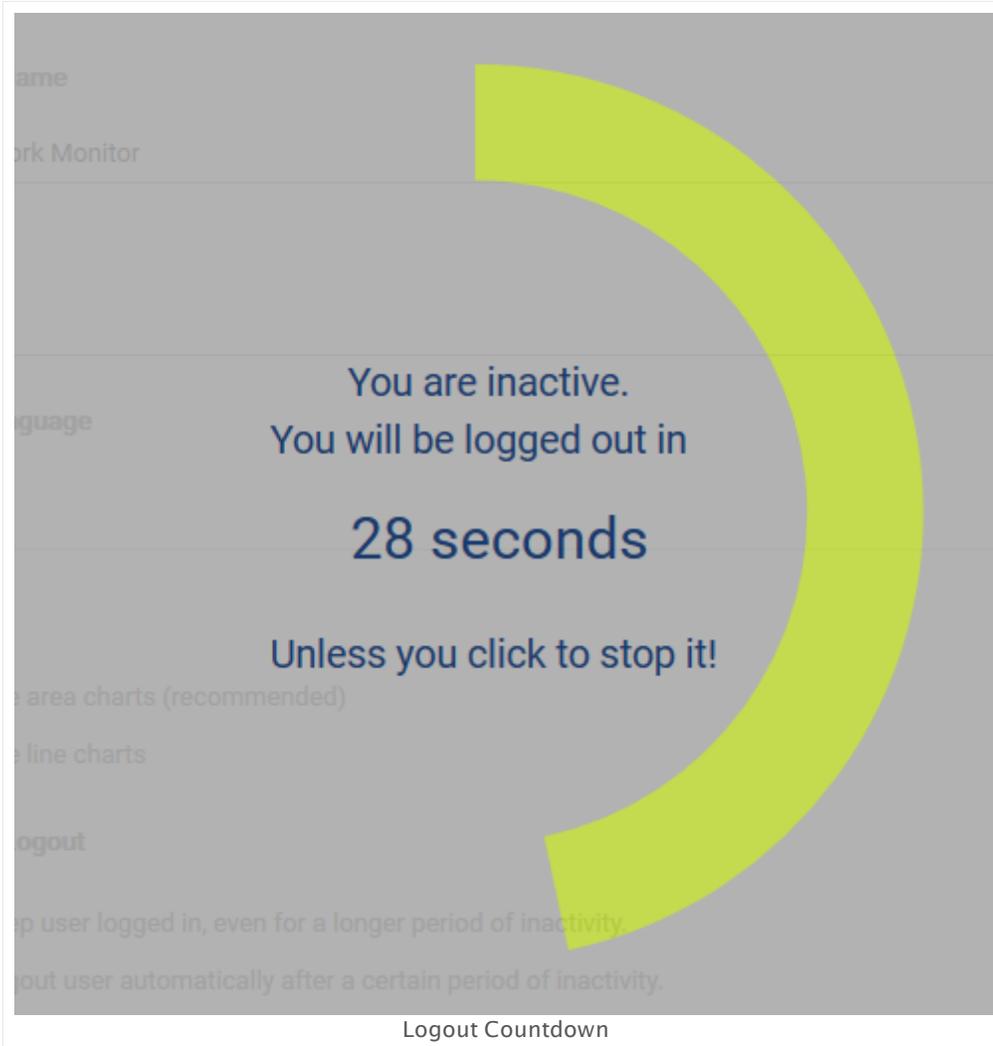
Automatic Logout Define if a user who is inactive for a certain period of time will be logged out from the PRTG interface automatically for security reasons. Choose between:

- **Keep user logged in, even for a longer period of inactivity.**
- **Logout user automatically after a certain period of inactivity.**

Automatic Logout after Minutes This field is only visible if you select the logout option above. Specify in minutes after which time of inactivity a user will be logged out automatically. Please enter an integer value. PRTG will redirect to the login page once this time has expired.

If the value you enter here is greater than 1 minute, a logout countdown will appear 1 minute before you are logged out. If the value is 1 minute, you will see the logout countdown 30 seconds before you are logged out. Click into the browser to stop the countdown and stay logged in.

WEBSITE



Google Analytics Tracking ID

You can track the usage of PRTG web pages with Google Analytics by entering your **Google Universal Analytics Tracking ID** into this field. You need a Google Analytics account for this feature. Create a tracking ID within the Google Analytics portal and provide it here. PRTG will then dynamically integrate it into the website.

Please enter a string or leave the field empty. The string will look like this: **UA-xxxxxx-xx**

 For details, see this Knowledge Base article: [How can I integrate Google Analytics in PRTG?](#)

 This option is not available in PRTG hosted by Paessler.

GEO MAPS

Map Service Provider	<p>Select if and how you want to integrate the Geo Maps feature into the web interface. If enabled, PRTG uses the first line of the location setting of an object^[217] to show it on a geographical map. Choose a map provider:</p> <ul style="list-style-type: none">▪ Do not show maps (disables Geo Maps integration): Disable Geo Maps integration and do not show geographical maps in the web interface.▪ Default (recommended): The recommended default option currently reroutes the map requests to Nokia Maps. See this blog article for details: Geo Maps Requires a Change of Map Service Provider▪ HERE Maps: Use HERE Maps to show geographical maps.▪ CloudMade (API key required): Use CloudMade to show geographical maps. Please sign up for an API key on their developer website to use this service.▪ Google Static Maps (API key required): Use Google Static Maps to show geographical maps. Please sign up for a Google Maps API v3 key to use this service as of PRTG version 13! <p> For more information about the different map providers, see this Knowledge Base article: Which provider should I use for PRTG's "Geo Maps" feature?</p>
Map Type	<p>This setting is only visible for some map providers. Depending on the chosen provider, several options are shown. Each will show map tiles in a different appearance. Choose a map type from the list.</p>
API Key (required)	<p>This field is only visible if you selected a provider that requires an API key. Obtain your personal key and paste it here.</p> <p> For more information on how to get a Google API key, see this Knowledge Base article: How do I get a Google Maps API key for use in PRTG?</p>

WEB SERVER

Performance Strategy	Select if you want to enable performance improvements for the web interface.
----------------------	--

WEB SERVER

- **All Features: Show all features and live data (recommended):** Provide full functionality and show all menu items.
- **More Speed: Limit features and delay display (experimental):** Improve reaction time and speed of the web interface by delaying display of monitoring data and hiding some features.

 For more information on how to speed up the web interface, see this Knowledge Base article: [How can I speed up PRTG—especially for large installations?](#)

IP Address for Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify the IP address this web server will run on. Later, you can log in to PRTG by simply pointing your browser to the specified IP address.

Choose between:

- **Localhost, 127.0.0.1 (PRTG will not be accessible from other computers):** Use **127.0.0.1** only. The PRTG web interface and the Enterprise Console will only be accessible from the computer PRTG is installed on. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on **127.0.0.1**.

 If you run PRTG on localhost, please do not use the DNS name **http://localhost** to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or **http://127.0.0.1** instead.

- **All IPs available on this computer:** Use all IP addresses available on this computer and enable access to the web server for all of these addresses. The TCP port selected below must be free on every available IP address.
- **Specify IPs:** Select specific IP addresses on which the PRTG Web server will run. A list specific to your system is shown. Add a check mark in front of every IP address you want the PRTG web server to be available at. You can also select and deselect all addresses by clicking on the check box in the table header. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.

 Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.

WEB SERVER

 If PRTG does not find a network card on startup it will switch the IP setting to **Localhost**. This setting will remain, even if a network card is available later on. If you disabled or removed the network card on the machine running the PRTG core server, please re-check this setting.

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [PRTG Apps for Mobile Network Monitoring](#)^[3484] will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

TCP Port for Web Server

PRTG runs a web server in order to provide access via the web interface and the Enterprise Console. Please specify on which port this web server will run. Choose between:

- **Secure HTTPS server (recommended, mandatory for internet access):** We recommend this setting and you need it to access the PRTG server via the internet. Use a secure HTTPS connection that is encrypted via SSL on port 443.

 Although the connection is secure, you will see an [SSL Certificate Warning](#)^[172] in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[3736].

 If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior by using a registry setting.

If port 443 is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG will send a [ticket](#)^[230] that shows you the currently used port number and will switch back to 443 as soon as it is available again.

- **Insecure HTTP server (standard port 80, not recommended):** Use a standard web server without SSL encryption on port 80. This setting is not recommended for WAN connections.

 If you use an insecure web server on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

WEB SERVER

- **Expert configuration:** This setting allows you to specify a custom web server port and the security of the connection. This option is intended for systems with an existing web server on the standard port. Define port and encryption below.

 If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft IIS web server also uses the port 80 (443 for SSL) by default and blocks it. Please disable such programs and services on startup.

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)³⁴³⁰, or of [PRTG Apps for Mobile Network Monitoring](#)³⁴⁸⁴ will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

Web Server Port

You will see this setting only if you select **Expert configuration** above. Enter the TCP port number you want the PRTG web server to run on. Please enter an integer value.

 If you use a secure connection and port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will be redirected to the custom port via HTTPS. You can change this behavior by using a registry setting.

 If the defined port for a secure connection is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG sends a [ticket](#)²³⁰¹ that shows you the currently used port number and will switch back to the original port as soon as it is available again.

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)³⁴³⁰, or of [PRTG Apps for Mobile Network Monitoring](#)³⁴⁸⁴ will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

WEB SERVER

Web Server Security

You will see this setting only if you select **Expert configuration** above. Specify if you want to use an SSL encryption. Choose between:

- **Use SSL encryption (HTTPS):** Use a secure HTTPS connection that is encrypted via SSL on a custom port as defined above.
 - ❗ Although the connection is secure, you will see an [SSL Certificate Warning](#)^[172] in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[3736].

- **Don't use encryption (not recommended):** This setting is not recommended for WAN connections. Use a standard web server without SSL encryption on a custom port as defined above.

⚠ If you use a web server without encryption on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

❗ If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [PRTG Apps for Mobile Network Monitoring](#)^[3484] will be disconnected and reconnected.

☁ This option is not available in PRTG hosted by Paessler.

SSL Security

Specify the security level that will be used for SSL connections from and to the PRTG web server. Choose between:

- **High security (recommended):** The web server will only accept high security connections from clients like web browsers, [apps](#)^[3484], the [Enterprise Console](#)^[3430], or API clients. These clients must be able to support modern ciphers that support authentication and encryption of **128 bits** or stronger and **forward secrecy**. All modern web browsers do this.
- **Weakened security (necessary for old web browser and old client software):** If you have clients that do not support the high security setting, you can choose this 'normal security level' setting to connect (for example, older browsers, browsers running on Windows XP, some default browsers on Android systems). However, we strongly recommend that you update your clients in this case.

WEB SERVER

 This option is not available in PRTG hosted by Paessler.

Currently Active IP
Address/Port
Combination(s)

Shows all currently active combinations of IP addresses and ports on which the PRTG server listens for web requests. This setting is shown for your information only and cannot be changed here.

 PRTG internally uses port 8085 for report generation.

 This option is not available in PRTG hosted by Paessler.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

PRTG shows several graphs in the [objects' detail pages](#)^[198] in the web interface. These are kept in RAM memory for fast display without causing extra CPU load or disk usage. The longer the time frames and the shorter the intervals are, the more memory will be used for this. You can adapt the details for all four graphs. This setting will also change the caption of the objects' tabs in the [web interface](#)^[166] and [Enterprise Console](#)^[3430].

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [PRTG Apps for Mobile Network Monitoring](#)^[3484] will be disconnected and reconnected.

Live Graph

The live graph is available for sensors only. For the live graph, no fixed time span is given, but you can define how many values will be displayed. The actual time span covered by the live graph depends on the scanning interval set for the sensor you're viewing and is calculated automatically. By default, **120 Values** is set, which results in a graph covering a time span of two hours, if a scanning interval of 60 seconds is set for the sensor. Other scanning intervals will result in graphs covering different time spans. Choose between:

- **60 Values:** This corresponds to a live graph covering a time span of one hour if a 1 minute scanning interval is set. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

- **120 Values:** This corresponds to a live graph covering a time span of two hours if a 1 minute scanning interval is set.
- **240 Values:** This corresponds to a live graph covering a time span of four hours if a 1 minute scanning interval is set.
- **480 Values:** This corresponds to a live graph covering a time span of eight hours if a 1 minute scanning interval is set.
- **960 Values:** This corresponds to a live graph covering a time span of 16 hours if a 1 minute scanning interval is set. Uses most RAM memory.

Graph 1

By default, this is the **2 days** graph in the web interface. You can change it to more or less detail by choosing a time span and a monitoring interval average associated with it. Monitoring results will be averaged regardless of the actual scanning interval set for the sensors. Choose between:

- **1 day with 1 minute averages:** Results in 1440 values.
- **1 day with 5 minutes averages:** Results in 288 values.
- **1 day with 15 minutes averages:** Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **2 days with 1 minute averages:** Results in 2880 values. Uses most RAM memory.
- **2 days with 5 minutes averages:** Results in 576 values.
- **2 days with 15 minutes averages:** Results in 192 values.
- **4 days with 1 hour averages:** Results in 96 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.

Graph 2

By default, this is the **30 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **10 days with 1 hour averages:** Results in 240 values.
- **20 days with 1 hour averages:** Results in 480 values.
- **30 days with 1 hour averages:** Results in 720 values.
- **30 days with 6 hour averages:** Results in 120 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.

GRAPH SETTINGS: SELECT FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

- **40 days with 1 hour averages:** Results in 960 values.
- **40 days with 6 hour averages:** Results in 160 values.
- **60 days with 1 hour averages:** Results in 1440 values. Uses most RAM memory.
- **60 days with 6 hour averages:** Results in 240 values.

Graph 3

By default, this is the **365 days** graph in the web interface. You can change it to more or less detail by choosing a time span covered and a monitoring interval average associated with it. Choose between:

- **100 days with 1 day averages:** Results in 100 values. Uses least RAM memory. We recommend this setting for installations with 10,000 sensors or more.
- **200 days with 1 day averages:** Results in 200 values.
- **365 days with 1 day averages:** Results in 365 values.
- **400 days with 1 day averages:** Results in 400 values.
- **750 days with 1 day averages:** Results in 750 values. Uses most RAM memory.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Knowledge Base: Which provider should I use for PRTG's "Geo Maps" feature?

- <https://kb.paessler.com/en/topic/34603>

Knowledge Base: Which domains and ports does the GeoMaps feature use?

- <https://kb.paessler.com/en/topic/35823>

Knowledge Base: How do I get a Google Maps API key for use in PRTG?

- <https://kb.paessler.com/en/topic/32363>

Knowledge Base: Which limitations apply when using the Google Maps API in PRTG?

Part 8: Ajax Web Interface—Advanced Procedures | 12 Setup
5 System Administration—User Interface

- <https://kb.paessler.com/en/topic/7913>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: How can I integrate Google Analytics in PRTG?

- <https://kb.paessler.com/en/topic/61406>

Paessler Blog: Geo Maps Requires a Change of Map Service Provider

- <https://www.paessler.com/blog/2016/07/12/all-about-prtg/geo-maps-requires-a-change-of-map-service-provider>

8.12.6 System Administration—Monitoring

In the monitoring settings you can define global values regarding scanning intervals, unusual and similar sensors detection, auto-discovery, and uptime threshold.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Monitoring Settings

ⓘ This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

SCANNING INTERVALS

☁ This option is not available in PRTG hosted by Paessler.

Available Intervals Define the intervals available in the dropdown list of [every object's settings](#)^[247]. In the text field, enter one value in each line. Use **s**, **m**, **h**, and **d** for defining seconds, minutes, hours, and days. By default, there are the following scanning intervals defined:

30s: 30 seconds

1m: 1 minute

5m: 5 minutes

10m: 10 minutes

15m: 15 minutes

30m: 30 minutes

1h: 1 hour

4h: 4 hours

6h: 6 hours

12h: 12 hours

1d: 1 day

SCANNING INTERVALS

 We recommend that you do not use intervals shorter than 10 seconds to prevent system overload. Intervals below 10 seconds are not officially supported! The maximum supported scanning interval is 10 days.

You can also define specific points in time to indicate when PRTG executes scanning actions. Enter up to 50 concrete UTC points in time according to the formula

@ UTC hh:mm, hh:mm

 Your local time may be different from the UTC time!

 For more information on how to set specific points in time as a scanning time for sensors, see this Knowledge Base article: [Can I set a sensor to run at a specific time?](#)

UNUSUAL DETECTION

The unusual detection can set sensors to an **Unusual status**¹⁹⁵ when there are values that are untypical for the time span in which they are measured. PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor will indicate this with the unusual status.

You can define the granularity of the unusual detection here (this means, how big the difference must be to cause an unusual status). If you disable the unusual detection (both settings to **Never**), sensors will never show an unusual status.

-  You can enable and disable unusual detection for specific devices, entire groups, and probes in the respective **Object Settings**²¹⁷.
-  Unusual detection requires sensor data from at least four weeks (28 to 34 days) to have enough data available for comparison. If there is less data available, the unusual status cannot be calculated.

Show Unusual When Define when a sensor shows the unusual status, comparing the weekday. If you enable the detection here, the average of the values that were measured on the day before is compared to the average of the same weekday in previous weeks. Choose between:

- **Never:** Disable unusual detection for weekday average.

UNUSUAL DETECTION

- **24h average is <80% or >120% of weekday average:** The average of the values measured on the day before is either lower than 80% or higher than 120% than usually on the same weekday.
- **24h average is <50% or >200% of weekday average:** The average of the values measured on the day before is either lower than 50% or higher than 200% than usually on the same weekday.
- **24h average is <20% or >500% of weekday average (recommended):** The average of the values measured on the day before is either lower than 20% or higher than 500% than usually on the same weekday.
- **24h average is <10% or >1,000% of weekday average:** The average of the values measured on the day before is either lower than 10% or higher than 1,000% than usually on the same weekday.
- **24h average is <1% or >10,000% of weekday average:** The average of the values measured on the day before is either lower than 1% or higher than 10,000% than usually on the same weekday.

For example, consider a traffic sensor that usually measures 100 MB average traffic on a weekday. If you choose the first option, it would show an unusual status if the average from the day before is below 80 MB or above 120 MB.

Show Unusual When

Define when a sensor shows the unusual status, comparing the hour-of-day. If you enable the detection here, the average of the values that were measured in the hour before is compared to the average of the same hour on the same weekday in previous weeks. Choose between:

- **Never:** Disable unusual detection for hour-of-day average.
- **Hourly average is <80% or >120% of hour-of-day average:** The average of the values measured in the hour before is either lower than 80% or higher than 120% than usually in this hour of this weekday.
- **Hourly average is <50% or >200% of hour-of-day average:** The average of the values measured in the hour before is either lower than 50% or higher than 200% than usually in this hour of this weekday.
- **Hourly average is <20% or >500% of hour-of-day average (recommended):** The average of the values measured in the hour before is either lower than 20% or higher than 500% than usually in this hour of this weekday.

UNUSUAL DETECTION

- **Hourly average is <10% or >1,000% of hour-of-day average:**
The average of the values measured in the hour before is either lower than 10% or higher than 1,000% than usually in this hour of this weekday.
- **Hourly average is <1% or >10,000% of hour-of-day average:**
The average of the values measured in the hour before is either lower than 1% or higher than 10,000% than usually in this hour of this weekday.

Consider a traffic sensor that usually measures 10 MB average traffic within an hour. If you choose the first option, it would show an unusual status if the average from the hour before is below 8 MB or above 12 MB.

Logging

Define if unusual events will be written to the logfile. Choose between:

- **Do not log unusual events**
- **Write unusual events into the log** (default)

SIMILAR SENSORS DETECTION

Similar sensors detection enables PRTG to analyze sensor data for similarities. The detection will run in the background with low priority. The recommended setting for similar sensors detection is to let PRTG automatically decide how many channels will be analyzed. However, you can also override this setting.

i When similar sensors analysis is turned off or you have exceeded 1,000 sensors and have chosen the automatic analysis depth option, the similar sensors entry will not be shown in the main menu bar.

Analysis Depth

Define the number of channels PRTG will analyze to detect similarities between sensors or turn the analysis off. Choose between:

- **Manage automatically based on sensor count (recommended):** The analysis depth depends on the total number of sensors you have configured. PRTG will analyze all channels for up to 500 sensors, and only the primary sensor channels for up to 1,000 sensors. If exceeding 1,000 sensors, the analysis will be turned off. This is the default setting in PRTG on premises.

SIMILAR SENSORS DETECTION

- **Analyze primary channels only:** Only the primary channels of sensors are analyzed. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 1,000 sensors.
- **Analyze all channels (higher CPU load):** Similarity detection is applied to all channels. Be aware of potentially high CPU load of PRTG when choosing this setting for more than 500 sensors.
- **Turn analysis off:** No similarity detection takes place. Choose this option if you are not interested in the analysis results or you want to keep the CPU load of PRTG at a minimum. This is the default setting in PRTG hosted by Paessler.

RECOMMENDED SENSORS DETECTION

With the sensor recommendation engine, PRTG can analyze devices in your network and suggest sensors that are still missing for a complete monitoring. The analysis runs with low priority in the background when you add a new device, when the last analysis was executed more than 30 days ago, or when you [manually start](#)^[214] it.

See the manual section [Recommended Sensors](#)^[213] for more information, for example, on [SNMP settings](#)^[214], on the [results](#)^[214] you get and on how you [add the suggested sensors](#)^[215].

.

 This option is not available in PRTG hosted by Paessler.

Detection Engine

Define if you want PRTG to analyze your devices to recommend useful sensor types. Choose between:

- **Manage automatically based on sensor count (recommended):** PRTG runs the detection engine for installations with up to 5,000 sensors by default. If you exceed this threshold, PRTG disables the detection engine for performance reasons. We recommend that you set this option so you do not miss any important monitoring data about your network, without risking to run into performance issues.
- **Always show recommendations:** PRTG always analyzes your devices even if your installation exceeds 5,000 sensors and you will never miss any suggestion to complete your monitoring. But if you enable this option, please keep in mind this setting in case you encounter performance issues.

RECOMMENDED SENSORS DETECTION

- **Turn recommendations off:** PRTG never recommends sensors. Select this option if you have performance issues with PRTG or if you do not want to see this information on [device overview tabs](#)^[198]. Moreover, you will not find the option **Recommend Now** in [device context menus](#)^[254] or on overview tabs anymore.

AUTO-DISCOVERY

Run Discovery At Define the time when PRTG automatically runs an [Auto-Discovery](#)^[282] in your network if you configured a daily or weekly **Discovery Schedule** in the [auto-discovery group settings](#)^[285]. Choose a full hour between **0:00** and **23:00**. We recommend that you choose a time when there is little user activity in your network, because auto-discoveries can produce a certain amount of load.

UPTIME THRESHOLD

Desired Minimum Uptime Define which uptime in percent PRTG regards as 100 percent. This setting affects the colors shown next to the sensor icons in reports. Select one of the predefined values between **90 %** and **99.999 %**.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

Knowledge Base: Can I set a sensor to run at a specific time?

- <https://kb.paessler.com/en/topic/3723>

8.12.7 System Administration—Notification Delivery

In the notification delivery settings, you can define global settings for notification delivery. If you do not want to use a specific notification method, just leave the respective fields empty.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Note

This section describes one of four steps to set up the notification system in PRTG. To complete your notification setup, go through all of the following steps:

1. Check and set up the **Notification Delivery** settings to define how and to which recipient PRTG will send messages.
For detailed information, see [System Administration—Notification Delivery](#) ³³⁶¹.
2. Check and set up **Notification Contacts** for the PRTG users to define the recipients of notifications.
For detailed information, see [Account Settings—Notification Contacts](#) ³³³⁴.
3. Check and set up **Notification Templates** to define the notification methods and their content.
For detailed information, see [Account Settings—Notification Templates](#) ³³¹¹.
4. Check and set up **Notification Triggers** for objects to define when notification messages will be sent.
For detailed information, see [Sensor Notification Triggers Settings](#) ³¹⁷⁰.

ⓘ We recommend that you always set up at least two notifications with different delivery methods for a notification trigger, for example, one [email notification](#) ³³¹⁷ and one [SMS notification](#) ³³²⁰. If delivery via email fails (due to an email server failure or other reasons), PRTG can still notify you via your smartphone. Simply set your latency setting to a [state trigger](#) ³¹⁷² and a notification via a delivery method other than the one for the first trigger. Or set up a second trigger with another notification for the corresponding object.

📖 For background information, see the [Notifications](#) ³²¹⁶ section.

Notification Delivery Settings

ⓘ This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

SMTP DELIVERY

SMTP Delivery Mechanism	<p>Define how PRTG sends emails using Simple Mail Transfer Protocol (SMTP). Choose between:</p> <ul style="list-style-type: none"> ▪ Direct delivery using built-in email relay server (default): Use the SMTP relay server built into PRTG. This server manages its own email queue. For each email, it looks up the target SMTP server via the MX record of the target domain, and send the email. ▪ Use SMTP relay server (recommended inside LANs/NATs): Set up your own SMTP relay server to send emails. Enter data below. ▪ Use two SMTP relay servers (primary and fallback server): Set up two own SMTP relay servers—one primary and one as fallback server. Enter data below. <p> When monitoring inside your NAT or LAN, it is often a good idea to use your own LAN-based relay server to deliver notification emails quicker.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
Sender Email	<p>Enter an email address to use as sender of all emails. This setting is global and applies to all email notifications by default. You can override the sender email in the settings of individual Notifications³³¹⁷.</p>
Sender Name	<p>Enter a name to use as sender of all emails. This setting is global and applies to all email notifications by default. You can override the sender name in the settings of individual Notifications³³¹⁷.</p>
HELO Ident	<p>Enter the HELO Ident for SMTP. This must be a unique name, preferably the DNS name of the machine running PRTG. See SMTP RFC 2821: The sender-SMTP must ensure that the domain parameter in a HELO command is a valid principal host domain name for the client host.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
SMTP Relay Server	<p>This field is only visible if you enable SMTP relay server above. Enter the IP address or DNS name of the SMTP relay server.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
SMTP Relay SMTP Port	<p>This field is only visible if you enable SMTP relay server above. Enter the port number the SMTP relay server is running on. Standard value is 25.</p>

SMTP DELIVERY

 This option is not available in PRTG hosted by Paessler.

SMTP Relay Authentication

This field is only visible if you enable SMTP relay server above. Select the kind of authentication required for the SMTP server. Choose between:

- **No authentication is required:** Use SMTP without authentication.
- **Use standard SMTP authentication:** Use standard authentication.
- **SASL authentication is required:** Use secure authentication via Simple Authentication and Security Layer (SASL).

 This option is not available in PRTG hosted by Paessler.

SMTP Relay User

This field is only visible if you enable SMTP authentication above. Enter a valid username.

 This option is not available in PRTG hosted by Paessler.

SMTP Relay Password

This field is only visible if you enable SMTP authentication above. Enter a valid password.

 This option is not available in PRTG hosted by Paessler.

Use Encrypted Connection

This field is only visible if you enable SMTP relay server above. Enter the security level for SMTP connections. Choose between:

- **Never:** Use insecure connection with plain text transfer.
- **If supported by server:** Use a secure connection (default).

 This option is not available in PRTG hosted by Paessler.

SSL Method

This setting is only visible if you enable SMTP relay server and encryption above. It is only relevant for secure connections. Select the SSL or TLS version that your SMTP device supports.

We recommend that you use the default value. If you do not get a connection, try with another setting. Choose between:

- **SSL V2 or V3**
- **SSL V3**
- **TLS V1**

SMTP DELIVERY

- **TLS V1.1**
- **TLS V1.2**

 This option is not available in PRTG hosted by Paessler.

SMTP Relay Server
(Fallback)

SMTP Relay SMTP Port
(Fallback)

SMTP Relay
Authentication
(Fallback)

Use Encrypted
Connection (Fallback)

These fields are only visible if you enable the option for two SMTP relay servers above. Please see also the settings that you made for your primary SMTP relay server.

SSL Method (Fallback)

SMTP Relay User
(Fallback)

 This option is not available in PRTG hosted by Paessler.

SSL Method (Fallback)

SMTP Relay User
(Fallback)

SMTP Relay Password
(Fallback)

Security (Fallback)

SMS DELIVERY

 Although PRTG has built-in support for the Application Programming Interface (API) of some SMS providers, we cannot officially provide support regarding these SMS service providers. If you have technical questions about SMS delivery beyond PRTG, please contact your SMS provider directly.

SMS DELIVERY

 Instead of using a pre-configured provider you can always use a custom URL, enabling you to use extended parameters (this is also an alternative when using providers for which we offer pre-configured options).

You need an internet connection to send text messages via the HTTP API.

 For information about sending SMS via separate hardware using third-party software, see this Knowledge Base article: [How can I send SMS text message notifications via a modem or a mobile phone with PRTG?](#)

Configuration Mode Define how you want to select an SMS provider. Choose between:

- **Select an SMS provider from a list of providers:** Select a provider from a list below.
- **Enter a custom URL for a provider not listed:** Use another provider and enter the service URL manually below.

Service Provider This field is only visible if you choose the provider list above. Select a service provider from the list. PRTG offers a small incomplete list of providers.

 Some providers might require a port configuration in your firewall. For details, see this Knowledge Base article: [Which URLs does PRTG use for its preconfigured SMS providers?](#)

User This field is only visible if you choose the provider list above. Enter a username for the service provider account.

Password This field is only visible if you choose the provider list above. Enter a password for the service provider account.

API ID / Account This field is only visible if you choose the provider list above. Some providers need an additional API ID or account information. If provided, enter it here. Please enter a string or leave the field empty.

Custom URL This field is only visible if you enable the custom provider option above. From the documentation of your SMS provider, enter the service URL that is used to send SMS messages.

Use the following placeholders for the recipient phone number and the text message:

- **%SMSNUMBER**
- **%SMSTEXT**

 Please use the **GET** method to request the custom URL. **POST** requests are not supported.

SMS DELIVERY

Custom URL-SNI	Select if PRTG will send the SNI extension to the TLS protocol along with the HTTP request. Choose between: <ul style="list-style-type: none">▪ Do not send SNI (default): PRTG will not send an SNI when executing the HTTP action.▪ Send SNI: PRTG will send an SNI when calling the target URL. Specify the SNI below.
Virtual Host (SNI)	This field is only visible if you select the SNI option above. Enter the SNI name that your endpoint configuration requires. Usually, this is the Fully Qualified Domain Name (FQDN) of the virtual host.
Encoding for SMS	Define the encoding of the URL string that PRTG sends to your provider. Choose between: <ul style="list-style-type: none">▪ ANSI local system codepage (default)▪ UTF-8▪ UTF-16
Maximum Length of Text	Some SMS providers will not allow SMS messages exceeding a certain amount of characters. PRTG will restrict the number of characters according to the length specified in this field. A value of 0 means the SMS is sent at its full length.

 The [notification](#)³³¹¹ methods **Send SMS/Pager Message** and **Execute HTTP Action** will use the central proxy settings defined for your PRTG core server. For details, see [System Administration—Core & Probes](#)³³⁶⁸ (section **Proxy Configuration**).

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

More

Knowledge Base: How can I send SMS text message notifications via a modem or a mobile phone with PRTG?

- <https://kb.paessler.com/en/topic/393>

Knowledge Base: Why do I get a connection timeout message when sending SMS via bulksms?

- <https://kb.paessler.com/en/topic/12253>

Knowledge Base: Which URLs does PRTG use for its preconfigured SMS providers?

- <https://kb.paessler.com/en/topic/13123>

Knowledge Base: How can PRTG send instant messages to Jabber, ICQ, MSN, Yahoo, etc., using external software?

- <https://kb.paessler.com/en/topic/14803>

Knowledge Base: Can GMail / Google Apps be used for SMTP relay?

- <https://kb.paessler.com/en/topic/2823>

Knowledge Base: How can I enable Notification Delivery Logging?

- <https://kb.paessler.com/en/topic/55363>

Knowledge Base: How can I include my own logo into HTML emails?

- <https://kb.paessler.com/en/topic/65782>

Knowledge Base: Can I use Microsoft Office 365 as SMTP relay server for PRTG email delivery)

- <https://kb.paessler.com/en/topic/75534>

8.12.8 System Administration—Core & Probes

In the core and probe management settings you can define settings for the core server, as well as the settings for probe connections if you use remote or mini probes.

i If you cannot save changes to **Core & Probes** settings because you get an **Error (Bad Request)** with the message **Active Directory Domain not accessible**, ensure you provide the correct access type for your domain in section **Active Directory Integration**³³⁷²! For example, change from "local user" to **Use explicit credentials** and provide correct credentials for the domain. Please note that PRTG automatically sets the access type "local system" by default, so you might need to change this.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Core and Probes Settings

i This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

PROXY CONFIGURATION

 This option is not available in PRTG hosted by Paessler.

Use Proxy Server	<p>We recommend that you use PRTG with a direct internet connection. However, if you need to use a proxy, you can configure the relevant settings here. Choose between:</p> <ul style="list-style-type: none"> ▪ No, use direct connection to the internet (default): Do not use a proxy. Use this setting if there is a direct internet connection available to the server running the PRTG core server. ▪ Yes, in our network a proxy is mandatory: Define proxy settings below. <p>i Proxy settings are valid for Auto-Update³⁴⁰⁷, Activate the Product⁹⁹, obtaining Geo Maps³²¹¹ tiles, and for sending out HTTP, push, and SMS text message Notifications³³¹⁶.</p>
Proxy Server	<p>This setting is only visible if proxy usage is enabled above. Enter the address of the proxy server that you use for outbound connections. Please enter a valid address.</p>

PROXY CONFIGURATION

Port	This setting is only visible if proxy usage is enabled above. Enter the port number of the proxy server that you use for outbound connections. Please enter an integer value.
Use Proxy Credentials	This setting is only visible if proxy usage is enabled above. Determine whether the proxy server needs credentials or not. Choose between: <ul style="list-style-type: none">▪ No, there are no credentials necessary: Do not use credentials for proxy connections.▪ Yes, the proxy server requires credentials: Define credentials (username and password) below.
User	This setting is only visible if proxy credentials are enabled above. Enter a username for proxy authentication. Please enter a string.
Password	This setting is only visible if proxy credentials are enabled above. Enter a password for proxy authentication. Please enter a string.

PROBE CONNECTION SETTINGS

Probe Connections IPs	Define how PRTG handles incoming connections from probes. Choose between the following options: <ul style="list-style-type: none">▪ Local Probe only, 127.0.0.1 (PRTG will not be accessible for Remote Probes): The PRTG core server^[126] only accepts local probe connections. You cannot use remote probes^[370] with this setting enabled. This is the default setting in PRTG on premises.▪ All IPs available on this computer: The PRTG server will always accept incoming connections from remote probes, no matter on which IP address of the core server they come in. This is the default setting in PRTG hosted by Paessler.▪ Specify IPs: The PRTG server will accept Incoming connections from remote probes^[371] only on the selected IP address(es) of the core server. In the list, select the IP addresses by adding a check mark in front of the desired IPs. <p> You can also change this setting in the PRTG Administration Tool on Core Server System^[356].</p>
-----------------------	---

PROBE CONNECTION SETTINGS

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)³⁴³⁰, or of [PRTG Apps for Mobile Network Monitoring](#)³⁴⁸⁴ will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

Access Keys

Enter a list of access keys, one per line. Every (remote) probe that wants to connect to this PRTG installation has to use one of these keys.

 For more information on how to set this key for a probe, see the [PRTG Administration Tool](#)³⁵⁸⁸ section.

Allow IPs

Enter a list of remote probe IPs or DNS names that will be accepted when connecting to this PRTG installation. Provide one IP address or DNS name per line. The local probe (**127.0.0.1**) is always allowed automatically. PRTG will check the list of allowed addresses first before the list of denied addresses.

- **[Empty]**: An empty field does not allow any remote probes (but only the local probe). Please enter IP addresses or DNS names to allow remote probe connections.

 We recommend that you use IP addresses rather than DNS names, because DNS name resolution may be cached.

- **any**: Enter the word **any** to automatically allow all remote probe connections. This is the default setting in PRTG hosted by Paessler.

 We recommend that you only use this option in intranets in PRTG on premises!

 If the IP address of your remote probe changes regularly (for example, due to an internet provider assigning IP addresses dynamically), please enter the potential IP range for this remote probe or use the **any** option.

 You can use the PRTG syntax for IP address ranges here. For more information, see the [Define IP Ranges](#)³⁶⁹² section.

PROBE CONNECTION SETTINGS

Deny IPs

Enter a list of remote probe IPs or DNS names that will **not** be accepted when connecting to this PRTG installation. Provide one IP address or DNS name per line. This is useful to explicitly deny connections from certain remote probes you do not want to include in your setup any more (for example, for a certain time).

Access to IP addresses or DNS names you allowed above will be denied if you enter them here. This is useful to allow access to an IP range in the field above, but deny access to a single IP address. You can use the PRTG syntax for IP address ranges here (see the [Define IP Ranges](#) section).

-  We recommend that you use IP addresses rather than DNS names, because DNS name resolution may be cached.

Deny GIDs

Enter a list of GIDs, one global ID (GID) per line. The access to matching GIDs will be denied. If you remove a remote probe from the device tree or if you deny a remote probe after installation, its GID will be automatically entered here. This specific remote probe will not be able to connect anymore. Denying GIDs is more precise than denying IPs, where other remote probes at the same location could be excluded too.

-  What is a global ID (GID)? It is the ID that PRTG Network Monitor attributes to every device that you include in your monitoring.

Mini Probes

Define if you want to allow Mini Probe connections to your PRTG server. If you want to use Mini Probes, you need to set up your PRTG web server to accept connections of Mini Probes here and choose the secure HTTPS server option in the [web server settings](#) section. Choose between:

- **No Mini Probes:** Mini Probes cannot connect to your PRTG web server. You are not able to monitor with Mini Probes if you choose this option.
- **Allow Mini Probes to connect to the web server:** Mini Probes can connect to your PRTG web server and use the [defined TCP port for the web server](#) for this purpose. The default port for SSL connections is **443**.
- **Allow Mini Probes to connect to an extra port:** Mini Probes can connect via a specific port to your PRTG web server. This is useful if you do not want to have your whole PRTG web server reachable from other networks all the time only because of Mini Probes.
 -  SSL is always required to be active on the Mini Probe port.

 See section [Mini Probe API](#) for the full Mini Probe documentation. See also this Knowledge Base article: [Where can I find PRTG Mini Probes which are ready to use?](#)

PROBE CONNECTION SETTINGS

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)³⁴³⁰, or of [PRTG Apps for Mobile Network Monitoring](#)³⁴⁸⁴ will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

Mini Probe Port

This field is only visible if you select the extra Mini Probe port option above. Enter the number of the port that you want to use for Mini Probe connections. Ensure that SSL is available on this port.

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#)³⁴³⁰, or of [PRTG Apps for Mobile Network Monitoring](#)³⁴⁸⁴ will be disconnected and reconnected.

 This option is not available in PRTG hosted by Paessler.

ACTIVE DIRECTORY INTEGRATION

 This option is not available in PRTG hosted by Paessler.

Domain Name

To use the [Active Directory Integration](#)³⁶⁰³ enter the name of your local domain. Please enter a string or leave the field empty.

 PRTG does not support trusted domains or AD subdomains. For more important notes about AD integration, see section [Active Directory Integration—Notes and Limitations](#)³⁶⁰⁴.

ACTIVE DIRECTORY INTEGRATION

Access Type	<p>Define which user account PRTG will use to configure Active Directory (AD) access. PRTG uses this account to query the AD for existing groups. Choose between:</p> <ul style="list-style-type: none">▪ Use the PRTG core service account (usually LOCAL SYSTEM): Use the same Windows user account configured for the "PRTG Core Server Service". In a default installation, this is the "local system" Windows user account. If this account does not have the right to query all groups of your Active Directory, do not use this option.▪ Use explicit credentials: Define a user account that PRTG will use to authenticate against the Active Directory. This should be a user account with full access to all of your Active Directory groups.
Access User	<p>This field is only visible if you enable the use of explicit credentials above. Enter the Windows user account name that PRTG will use to authenticate for Active Directory configuration.</p>
Access Password	<p>This field is only visible if you enable the use of explicit credentials above. Enter the password for the Windows user account that PRTG will use to authenticate for Active Directory configuration.</p>

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Data purging enables you to automatically delete unnecessary data to free up disk space and improve system performance. You can define different time spans for several kinds of data. Select here for how many days historic data remains accessible.

 For further information on storage locations, see the [Data Storage](#)  section.

 This option is not available in PRTG hosted by Paessler.

 PRTG hosted by Paessler purges historic data using the default purging limits of PRTG on premises (see the table below). You cannot modify historic data purging limits in PRTG hosted by Paessler.

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Logfile Records Define how long records in the system logfile **Log Database.db** will be kept. Enter a value in days. All entries older than this value will be deleted from the logfile automatically. This also affects the content of the **Logs**^[228] tab of monitoring objects like sensors. Keep this value as low as possible to enhance system performance.

 Default value is **30** days.

Web Server Log Records PRTG creates one web server logfile every day. Define how many web server logfiles are kept. Enter a value in days. All web server logfiles older than this value will be deleted automatically.

 Default value is **30** days.

Historic Sensor Data Define for how many days historic sensor data are kept for all sensors. It is used to create **reports**^[3252] of monitoring data. Enter a value in days.

Depending on the used intervals and the number of sensors in your setup, the file containing this data can become large. For smaller installations (500 sensors or less) a value of 365 is usually fine.

 Historic sensor data is the basis for reports on monitoring data. If you decrease this value, there will be less historic monitoring data available!

 Default value is **365** days.

Toplist Records Define how long toplist records for **Flow**^[3514] and **Packet Sniffer**^[3512] sensors are kept. Enter a value in days. We recommend using 30 days here.

 Old toplist data will be purged automatically as soon as a limit of 2 GB is reached. The oldest data is deleted first from the database.

 Default value is **30** days.

Closed Tickets Define how long tickets that are in status **closed** are kept. Enter a value in days.

 Default value is **365** days.

HISTORIC DATA PURGING: DEFINE FOR HOW MANY DAYS HISTORIC DATA REMAINS ACCESSIBLE

Reports	<p>Reports generated in PDF format are stored on disk for later reference. Define the maximum age for these reports. Enter a value in days. All reports older than this value are deleted automatically.</p> <p> Default value is 365 days.</p>
Configuration Auto-Backups	<p>PRTG creates one backup of your configuration every day. Define the maximum age for these backups. Enter a value in days. All configuration backup files older than this value will be deleted automatically.</p> <p> Default value is 365 days.</p>
Full HTTP Sensor Screenshots	<p>Define how long the screenshots of the HTTP Full Web Page Sensor¹⁰²⁷ (PhantomJS browser engine) are kept. Enter a value in days. PRTG will delete older screenshots with every sensor scan.</p> <p> Default value is 10 days.</p>

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Remote Probe Setup

Find more information about setting up remote probes in the [Multiple Probes and Remote Probes](#)³⁷⁰⁷ section.

More

- [Define IP Ranges](#)³⁶⁹²

Knowledge Base: Where can I find PRTG Mini Probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

8.12.9 System Administration—User Accounts

PRTG administrator users can change all user account settings and add new users.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

User Accounts Overview

The **User Accounts** tab shows a list of all user accounts that exist on this PRTG server. The **Users** table shows various information about each user at a glance.

- **Object**: the name of the user account. Click it to open the [User Account Settings](#)³³⁷¹.
- **Type**: the account type, for example, PRTG **Administrator** user or **Read Only User**
- **Email**: the **Primary Email Address** of this user account
- **Primary Group**: the Primary Group of this user account. Click it to open this [user group's settings](#)³³⁸¹.
- **Group Memberships**: all user groups that contain this user account
- **Active/Paused**: the status of this user account

■ See also section [Working with Table Lists](#)²³⁷¹ for more information.

You have several options to manage user accounts and groups on this page:

- To change a user's settings, select it from the list by clicking the username. The available setting options are the same as shown in the [My Account](#)³³⁰⁴ settings of the currently logged in user (plus some account control options).
- To add a new user to PRTG on premises, hover over  and select **New User** from the menu. The options are the same as for existing users (with slight differences).
- To add a new user to PRTG hosted by Paessler, click the **Invite User** button. The options are almost the same as for existing users, but the initial login password will be generated automatically. The new user can change it later. Click **Send Invite** to save your settings and to send the invitation per email to the defined **Primary Email Address**.
- To batch-add several users at once in a simple way, hover over  and select **Add Multiple Users** from the menu. In the dialog box that appears, select an existing [user group](#)³³⁸³ from the dropdown menu and enter or paste a list of email addresses. They can be separated by a space, comma, semicolon, or a new line. Click the **OK** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group to PRTG on premises, hover over  and select **Add User Group** from the menu. The options are the same as for existing groups (with slight differences).
- To add a new user group to PRTG hosted by Paessler, hover over the **Add User Group** button.

- Access rights in PRTG are given via user groups. Please make sure a user account is member of the correct [user group](#)^[3383] and give access to this group in your device tree [object's settings](#)^[217].

 Predefined objects cannot be deleted!

User Accounts Settings

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

USER ACCOUNT

Login Name	<p>Enter the login name for the user.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
Display Name	<p>Enter a name that the user recognizes. It will not be used for login purposes.</p>
Primary Email Address	<p>Enter the user's email address.</p> <p> Please use an email client that can show HTML emails, otherwise you cannot read emails from PRTG.</p>
Password	<p>Define the user password. For security reasons, the account settings page does not contain the password. Choose between:</p> <ul style="list-style-type: none"> ▪ Don't change ▪ Specify new password <p>If you choose to specify a new password, enter the old password and then the new password twice.</p> <p> The new password must be at least 8 characters long. It must contain a number and a capital letter. Leading and trailing whitespaces will be cut. The password of a PRTG Administrator user can only be changed by the same PRTG Administrator user.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
Passhash	<p>Click Show passhash to display the passhash for the selected user. You need the passhash of a user if you use the PRTG Application Programming Interface (API)^[3606]. This setting is shown for your information only and cannot be changed here.</p>

USER ACCOUNT

 This option is not available in PRTG hosted by Paessler.

API ACCESS

 These settings are only available in PRTG hosted by Paessler.

API Username Shows the username of the current user account. You need a username if you use the PRTG [Application Programming Interface \(API\)](#). This setting is shown for your information only and cannot be changed here.

API Passthrough Click **Show passthrough** to display the passthrough for the selected user. You need the passthrough of a user if you use the PRTG [Application Programming Interface \(API\)](#). This setting is shown for your information only and cannot be changed here.

Reset API Passthrough Click **Generate new passthrough** to reset the passthrough of the current user.

ACCOUNT CONTROL

Account Type This setting is only visible to administrator users. However, it will not show if the user whose account you want to modify is a member of a group with administrative rights.

Define the account type for the current user. Choose between:

- **Read/Write User:** You can change settings.
- **Read Only User:** You cannot edit any settings except your own password. This is a good choice for public or semi-public logins.

 This setting cannot be changed for the default administrator user.

ACCOUNT CONTROL

Allow Acknowledge Alarms

This setting is only visible if **Read Only User** is enabled above. Acknowledging an alarm is an action that requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may [acknowledge alarms](#)²²⁰. Choose between:

- **Allow:** Allow acknowledging alarms for this user.
- **Deny:** The user will not be able to acknowledge alarms.

Password Changes

Decide if you want the user to be able to change their account's password or not. If you allow the user to change the password, this option will be available in the [My Account](#)³³⁰⁴ settings of the respective user. Choose between:

- **User may change the account password**
- **User may not change the password** (default)

i This field is only visible if you edit this option for read-only users as an administrator.

Primary Group

This setting is available only for administrator users. Select the primary group for the current user. Every user has to be member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional. For user experience there is no difference between the primary and other user groups.

i You cannot change the primary group of **Active Directory** users. Users that you added with [Active Directory Integration](#)³⁶⁰³ can only have this AD group as their primary group. If you need to change this, please delete this user account and add it again.

Status

This setting is only shown for administrator users. Define the status of the current user. Choose between:

- **Active:** The current user can login to the account.
- **Inactive:** The current user's login is disabled. Use this option to temporarily deny access for this user.

i This setting cannot be changed for the default administrator user.

Last Login

Shows the time stamp of the user's last login. This setting is shown for your information only and cannot be changed here.

USER GROUPS

Member of Shows the groups the current user is member of. Access rights to the device tree are defined on group level. This setting is shown for your information only and cannot be changed here.

WEB INTERFACE

Auto Refresh Define if you want PRTG to reload web pages automatically for the current user. Choose between:

- **Refresh pages (recommended):** Automatically refresh the single page elements on the web pages in PRTG.
- **No automatic refresh:** Do not automatically refresh web pages.

Auto Refresh Interval (Sec.) This setting is only relevant if you enable auto refresh above. Enter the number of seconds that PRTG waits between two refreshes. We recommend that you use **30** seconds or more. Minimum value is 20 seconds.

 Shorter intervals create more CPU load on the server running PRTG. If you experience load problems while using the web interface (or PRTG [maps](#)^[3278]), please set a higher interval.

Play Audible Alarms Define when PRTG will play an audible alarm the current user on web pages whenever there are new [alarms](#)^[219]. Choose between:

- **Never:** Do not play sound files on any web pages.
- **On dashboard pages only:** When there are new alarms, play a predefined sound on [dashboard](#)^[263] pages only. The sound will be played with every refresh of the dashboard page if there is at least one new alarm.
- **On all pages:** When there are new alarms, play a predefined sound on all web pages. The sound will be played with every page refresh if there is at least one new alarm.

 Audible alarms are only played if the **New Alarms** value in the [Global Header Area](#)^[183] of the PRTG web interface is greater than 0 after a page refresh. The number of existing alarms is not considered.

 For more information about audible notifications and supported browsers, see this Knowledge Base article: [Which audible notifications are available in PRTG? Can I change the default sound?](#)

WEB INTERFACE

Homepage URL	Define the user's default page, which is loaded after logging in or clicking on the Home ²⁶³ button in the main menu.
Timezone	Define the time zone for the current user. Depending on the time zone you select here, PRTG shows the current user's local time zone in all data tables and graph legends. <i>i</i> PRTG receives the UTC (Coordinated Universal Time) from the system time set on the PRTG core server for this purpose.
Date Format	Define the date format for the current user. <i>i</i> This setting will take effect after the next login.
Color Mode	Select a color mode for your web interface.

TICKET SYSTEM

Email Notifications	Define if you want to get emails from the ticket system. Choose between: <ul style="list-style-type: none"> ▪ I want to receive an email whenever a ticket changes: You will receive an email each time a ticket is assigned to you or your user group, or if a ticket that is assigned to you or your user group is changed. <i>i</i> If you edit tickets that are assigned to you or your user group, or you assign a ticket to yourself or your user group, you will not get an email. ▪ I do not want to receive any emails from the ticket system: You will not get any emails about tickets.
---------------------	---

Notification Contacts

In the [Notification Contacts](#) ³³³⁴ tab you can define recipients for each user account. Recipients can be email addresses, phone numbers, or push devices (iOS and Android devices with the corresponding [PRTG smartphone app](#) ³⁴⁰⁴).

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Save your settings. If you leave the current page, all changes to the settings will be lost!

More

Knowledge Base: Which audible notifications are available in PRTG? Can I change the default sound?

- <https://kb.paessler.com/en/topic/26303>

8.12.10 System Administration—User Groups

The PRTG administrator users can change existing user groups or add new ones, and define the users that are member of a certain group.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

All the security settings as well as further rights management are conducted via the user groups. This means that group membership controls what a user may do and which objects the user will see when logged in. The actual rights for each object can be defined in an object's settings. There, you can define different rights for each user group.

The **User Groups** table shows you all existing user groups with various information at a glance. You can see all **Members** of a group as well as all user accounts that have this group as **Primary Group** or as **Active Directory Group**.

- To change a user group's settings, select it from the list by clicking on the group name.
- To add a new user to PRTG on premises, hover over  and select **New User** from the menu. The options are the same as for existing users (with slight differences).
- To add a new user to PRTG hosted by Paessler, click the **Invite User** button. The options are almost the same as for existing users, but the initial login password will be generated automatically. The new user can change it later. Click **Send Invite** to save your settings and to send the invitation per email to the defined **Primary Email Address**.
- To batch-add several users at once in a simple way, hover over  and select **Add Multiple Users** from the menu. In the dialog box that appears, select an existing [user group](#)³³⁸³ from the dropdown menu and enter or paste a list of email addresses. They can be separated by a space, comma, semicolon, or a new line. Click the **OK** button to confirm. For each address, PRTG will create a new local user account within the selected user group, carrying the email address as value for **Login Name**, **Username**, and **Email Address**. A new password will be generated automatically and sent to the email address.
- To add a new user group to PRTG on premises, hover over  and select **Add User Group** from the menu. The options are the same as for existing groups (with slight differences).
- To add a new user group to PRTG hosted by Paessler, hover over the **Add User Group** button.
- For each user group you create, PRTG automatically adds a new [device group](#)¹³⁴ with the name **[group_name] home** to the device tree.
- For each user group you create, PRTG automatically adds a new [email notification](#)³³¹⁷ to [notifications](#)³²¹⁶ with [read access rights](#)¹⁵⁸ for this user group. It has the name **Email to all members of group [group_name]**.

- By default, there are no [access rights](#)^[158] on existing objects for a newly created PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree except the automatically created **home** group (with write access rights). Please edit the [object settings](#)^[217] in your device tree and set access rights for your newly created user group in the **Inherit Access Rights** section.
 - ❗ The easiest way is to set these rights in the [Root Group Settings](#)^[331].
- ❗ The multi-edit option is not available for the standard user groups PRTG Administrators and PRTG Users Group.
- ❗ Predefined objects cannot be deleted!
- ❗ If you want to delete an Active Directory group, you have to delete all users that are in this group in PRTG first. This is because users that you add with [Active Directory Integration](#)^[3603] always have this group as their primary group.

User Groups Settings

- ❗ This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

USER GROUP SETTINGS

User Group Name	Enter a name for the user group.
Administrative Rights	<p>Define if the members of this group will be PRTG administrators. If you enable this option, all members of this group will have full access to all monitoring objects, maps, reports, user accounts and user groups, and they can change the PRTG monitoring configuration. Choose between:</p> <ul style="list-style-type: none"> ▪ Yes: Give full PRTG administrator rights to all members of this group. ▪ No: Do not make members of this group administrators. Access to monitoring objects for users that are member of this group will be controlled by the Access Rights settings defined in the Object Settings^[217] of Probes, Groups, Devices, or Sensors. <p>❗ This option is especially useful in combination with the Active Directory option below.</p>

USER GROUP SETTINGS

Default Homepage	Enter a PRTG internal web page. This will set the default homepage for all new users created with this group. A user will be redirected to this page after logging in. This concerns new users either added by an Active Directory login or by the Add multiple users feature.
Use Active Directory	<p>Define if this PRTG user group will be connected to a group in your active directory. Choose between:</p> <ul style="list-style-type: none">▪ Yes: Connect this group to an AD group. Choose below. For detailed information, see Active Directory Integration³⁶⁰³.▪ No: Do not use Active Directory integration for this group, but choose local user accounts instead. <p> This option is not available in PRTG hosted by Paessler.</p>
Active Directory Group	<p>If a valid Active Directory Domain is set in the System Administration—Core & Probes³³⁷² settings and Active Directory integration is enabled above, a dropdown menu will appear, showing the groups in your Active Directory. Choose the group whose members will be able to log in to PRTG using their Active Directory domain credentials. All of those AD users will be in the security context of the PRTG group you're about to create/edit.</p> <p> For detailed information, see Active Directory Integration³⁶⁰³.</p> <p>If your Active Directory contains more than 1000 entries in total, PRTG will display an input field instead of a dropdown menu. This is done due to performance reasons. In the input field, you can enter the group name only. PRTG will then add the prefix automatically.</p> <p> This option is not available in PRTG hosted by Paessler.</p>
New User Type	<p>If Active Directory integration is enabled above, define the default rights for all new users in this user group. If a user logs in for the first time using Active Directory credentials, PRTG will automatically create a new local user account for this user, applying the user type defined here. Choose between:</p> <ul style="list-style-type: none">▪ Read/Write User: The user may change settings.▪ Read Only User: The user may not edit any settings except the own password. This is a good choice for public or semi-public logins.

USER GROUP SETTINGS

Acknowledge Alarms	<p>This setting is only visible if Read Only User is enabled above. Acknowledging an alarm is an action that requires write access rights. However, you can explicitly allow this action to read-only users. If enabled, they still do not have write access, but may acknowledge alarms^[220]. Choose between:</p> <ul style="list-style-type: none">▪ User may acknowledge alarms: Allow read-only users to acknowledge alarms.▪ User may not acknowledge alarms (default): Read-only users will not be able to acknowledge alarms.
Allowed Sensors	<p>Define if members of this user group will be able to create all available sensor types or only specific ones. Choose between:</p> <ul style="list-style-type: none">▪ Users may always create all sensor types: No restrictions for group members are applied.▪ Users may create certain sensor types only: Choose the allowed sensor types below. This option is especially interesting for a Managed Service Provider (MSP).
Users May Create These Sensor Types	<p>This field is only visible if you defined that the users in this group are only allowed to create certain sensor types. A list of all available types is shown with their name. Select the desired types by adding check marks in front of the respective lines. You can also select and deselect all items by using the check box in the table head.</p>
Ticket System Access	<p>Define if the members of this user group will be able to use the PRTG ticket system^[230]. Choose between:</p> <ul style="list-style-type: none">▪ Members can use the Ticket System: No restrictions for group members are applied.▪ Members can NOT use the Ticket System: The Tickets^[274] option in the main menu bar^[274] will not be visible to users in this group.

MEMBERS

Members	<p>This setting is only available if Active Directory integration is disabled above. Define which local user accounts will be a member of this group. To add a user account from the list, add a check mark in front of the username. The user accounts available depend</p>
---------	--

MEMBERS

on your setup.

PRIMARY USERS

User List

Shows a list of all user accounts with this group set as primary group. This is shown for information purposes only. You can change it in a [user account's settings](#)³³⁷⁶.

Comments

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

History

In the **History** tab all changes in the settings of an object are logged with a timestamp, the name of the PRTG user who made the change, and a message. The history log retains the last 100 entries.

Save your settings. If you leave the current page, all changes to the settings will be lost!

8.12.11 System Administration—Administrative Tools

With the administrative tools you can start system specific processes for debugging purposes. Use them if our technical support advises you to do so. You can start the respective processes by clicking the **Go!** button.

■ If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Core Administrative Tools

The screenshot displays the 'Core Administrative Tools' section of the PRTG web interface. It features a navigation menu at the top with options like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this, there are sub-tabs for User Interface, Monitoring, Notification Delivery, Core & Probes, User Accounts, User Groups, and Administrative Tools. The main content area is titled 'Core Administrative Tools' and contains several tool cards, each with a 'Go!' button:

- Create Configuration Snapshot:** Saves current configuration as ZIP file in the 'Configuration Auto-Backups' folder.
- Write Core Status File:** Creates a debug file on the core system.
- Clear Caches:** Clears the web server's internal caches for Geo Maps and Active Directory authentication.
- Load Lookups and File Lists:** Reloads the lookup files from the 'lookups/custom' folder and other file lists that are displayed in the web interface, for example, SNMP libraries, device icons, and report templates.
- Recalculate PRTG Graph Data Cache:** Note: due to the recalculation the PRTG Core Server Service will be restarted.
- Restart Core Server:** Restarts the PRTG Core Server Service.
- Reload Logging Configuration:** Apply changes of the Logging Configuration to all PRTG Modules.

A note at the bottom of the page states: "Want to schedule a regular restart of the core server? Please go to the device tree and open the Settings of the Local Probe. In the Scheduled Restart Settings, edit the Restart Options."

PRTG Core Administrative Tools

CORE ADMINISTRATIVE TOOLS

Create Configuration Snapshot

Create a snapshot of your PRTG configuration. This action can take up to 100 seconds. Once finished, you will find a ZIP file that contains a ***.dat** file in the **Configuration Auto-Backups** subfolder of your [PRTG data directory](#)^[3734]. If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. The ZIP file follows the name pattern **PRTG Configuration (Snapshot YYYY-MM-DD HH-MM-SS).zip**.

☁ This option is not available in PRTG hosted by Paessler.

CORE ADMINISTRATIVE TOOLS

Write Core Status File Create status files of your PRTG core server. You will find the two text files in the **Logs (System)** sub folder of your [PRTG data directory](#)^[3734]. If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. The files are named **Core Status.txt** and **Core Memory.txt**. They are overwritten each time you click this button.

 This option is not available in PRTG hosted by Paessler.

Clear Caches PRTG caches tiles for [Geo Maps](#)^[3211] and user data for [Active Directory Integration](#)^[3603]. Use this button to delete the cache if you encounter broken Geo Maps tiles, or if you changed a user's password in the Active Directory.

 This option is not available in PRTG hosted by Paessler.

Load Lookups and File Lists (Re)load the [lookup files](#)^[3693] from the `\lookups\custom` folder. In this folder your customized lookup files are stored. If you have created a new lookup file or changed something in an existing lookup file, it might be necessary to load or to reload these files.

With this option, you can also manually reload file lists in the PRTG web interface. If you have added new [device icons](#)^[403], [device templates](#)^[3203], [report templates](#)^[3259], OIDlib files for the [SNMP Library sensor](#)^[2237], or language files to the PRTG program directory on the PRTG core server system while the server was running, reloading the file lists might be necessary to display new files in the web interface.

 Usually you will not have to reload file lists manually. A list will be automatically reloaded when opening the according settings page with a latency of 10 seconds. If you save new device templates via the web interface, the template list will be refreshed immediately.

 This option is not available in PRTG hosted by Paessler.

Recalculate PRTG Graph Data Cache

PRTG constantly writes monitoring data to disk and keeps the graphs for your graph tabs in memory. If PRTG is ended unexpectedly, the graph cache may get corrupted. In this case, graphs may be shown empty or show wrong data.

If you experience graph display problems, a graph recalculation will fix the problem. Click **Go!** to delete the data cache file and recalculate it automatically.

CORE ADMINISTRATIVE TOOLS

 If you apply recalculation, PRTG needs to restart the core server. Because of this, all users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [Smart phone Apps](#)^[3484] will be disconnected. After clicking the **Go!** button, a dialog window will appear that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen.

 Directly after this action your graphs will be empty. They will be re-filled successively while recalculation in the background progresses. Until recalculation is finished, performance of the PRTG web interface may be affected due to high disk I/O activity.

Restart Core Server

Restart the PRTG core server service manually. Click the **Go!** button for this purpose.

 If you restart the core server, all users of the PRTG web interface, of the [Enterprise Console](#)^[3430], or of [Smart phone Apps](#)^[3484] will be disconnected. After clicking the **Go!** button, a dialog window will appear that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen.

 If you want to schedule an automatic restart of Windows services for both core server and probe service, you can do this in the corresponding [Probe Settings](#)^[371].

 This option is not available in PRTG hosted by Paessler.

Reload Logging Configuration

For debugging reasons it might be necessary to change the log levels of your PRTG instance. The Paessler Support Team will take you through the necessary steps that are required to change your logging configuration. The log level changes will vary according to your PRTG instance, its setup, and the solution of your issue.

To apply the changes to your PRTG logging, load them by clicking **Go!**.

Probe Administrative Tools

Probe Administrative Tools

Write Probe Status Files

Creates a set of debug files on all probe systems.

Restart All Probes

Restarts all probe services. For disconnected probes, please use the PRTG Administration Tool on the respective probe system to start the probe service.

Probe #1 "Local Probe"

connected from: 127.0.0.1:60983
 Last Data: 20.06.2018 21:14:01 (0 sec ago) (Mittleeuropäische Zeit)
 .NET Framework Support: Installed: v4\Client (4.5.51641), v4\Full (4.5.51641), v4.0\Client (4.0.0.0)

Want to schedule a regular restart of a remote probe? Please go to the device tree and open the Settings of the respective remote probe. In the Scheduled Restart Settings, edit the Restart Options.

PRTG Probe Administrative Tools

PROBE ADMINISTRATIVE TOOLS

Write Probe Status Files

Create status files of your PRTG probes. PRTG writes status files for the local probe running on the PRTG core server (if you run a PRTG cluster, on the cluster node you are currently logged in to) as well as for all remote probes configured (if any).

On the respective systems, you will find four text files in the **Logs (System)** sub folder of the [PRTG data directories](#)³⁷³⁴. The files follow the name pattern **Probe Memory XX.txt**, **ProbeState XX.txt**, **ProbeState AXX.txt**, and **ProbeState BXX.txt**. They are overwritten each time you click this button.

Restart All Probes

Restart all PRTG probes as well as the local probe Windows service. If there are any [remote probes](#)³⁷⁰⁷ configured, the probe Windows services on the respective remote systems will be restarted as well. To restart single probes only, see below.

 Disconnected probes cannot be restarted here. Please use the [PRTG Administration Tool](#)³⁵⁶⁰ on the probe system to start a disconnected probe.

PROBE ADMINISTRATIVE TOOLS

 If you run a PRTG cluster, this action is executed on the cluster node you are currently logged in to. In this case, remote probes are only restarted if you are logged in to the primary master node. The cluster probe Windows service of failover nodes is not restarted if you execute this action on the master node. If you want to restart the cluster probe Windows service of a failover node, please log in to this failover node's web interface and click the **Go!** button there.

Probe [#Number]
"[Name]"

This section shows information about the connection status. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the **Local Probe**, the IP will always be 127.0.0.1. You will also see information about the date when the last data packet was received from the probe.

If you want to restart a single probe, click the corresponding **Restart Probe** button. Entries for every single probe are following.

 Disconnected probes cannot be restarted here. Please use the [PRTG Administration Tool](#)³⁵⁶⁰ on the probe system to start a disconnected probe.

 This option is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

Setup—Topics

- [Account Settings—My Account](#)  3304
- [Account Settings—Notification Templates](#)  3311
- [Account Settings—Notification Contacts](#)  3334
- [Account Settings—Schedules](#)  3338
- [System Administration—User Interface](#)  3343
- [System Administration—Monitoring](#)  3355
- [System Administration—Notification Delivery](#)  3361
- [System Administration—Core & Probes](#)  3368
- [System Administration—User Accounts](#)  3376
- [System Administration—User Groups](#)  3383
- [System Administration—Cluster](#)  3394
- [System Administration—Administrative Tools](#)  3388
- [PRTG Status—System Status](#)  3396
- [PRTG Status—Auto-Update](#)  3407
- [PRTG Status—Cluster Status](#)  3412
- [PRTG Status—Activation Status](#)  3414
- [Downloads and Tools](#)  3420
- [Desktop Notifications](#)  3422
- [Support—Contact Support](#)  3424

Others

There are some settings that you must make in the [PRTG Administration Tool](#)  3560, available as native Windows application. For more details, see the sections:

- [PRTG Administration Tool on Core Server System](#)  3561
- [PRTG Administration Tool on Remote Probe System](#)  3567

8.12.12 System Administration—Cluster

In the cluster settings you can define the cluster settings. During [Failover Cluster Configuration](#)^[3720], the cluster settings were already pre-defined. See the [cluster status](#)^[3412] to see if all nodes in your cluster are properly connected.

 This feature is not available in PRTG hosted by Paessler.

 If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

Cluster Settings

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

You can set up two, three, four, or five nodes in one cluster for PRTG on premises. In the table of the cluster settings, the information of each node is written in one line.

CLUSTER NODE SETUP

Node Name	Enter the name of the node (for display purposes).
Node ID	The ID is unique for every node. We recommend that you use the default value.
Node State	<p>You can set the state for every failover node. Choose between:</p> <ul style="list-style-type: none"> ▪ Active: Set the node to be active. ▪ Inactive: Set the node to be not active. It will be disabled in the cluster configuration. It will then be not an active part of the cluster and will not appear in the cluster status^[3412] any more. <p> This setting is not available for the master node of a cluster. The master is always set to Active.</p>
IPs/DNS Names Used for Connections Between Nodes	Define the IP addresses or DNS names that will be used for the connections between the nodes. You can enter different values for every node-node connection.

CLUSTER NODE SETUP

For example, in the field #2 => #1, enter the address under which the master node server can be reached from the second cluster member. Usually, this is the IP address or DNS name of the master node. Do this for all available node connections, for example, if you run three nodes, enter the address under which second node can be reached from the third cluster member into the field #3 => #2.

 See also section [Failover Cluster Step by Step, Step 4](#)  and following.

 If you use [remote probes](#)  outside your local network or outside your Network Address Translation (NAT), ensure the IP addresses or DNS names you enter here are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. These addresses must not be private and have to be reachable from the outside, otherwise your remote probes will not be able to connect.

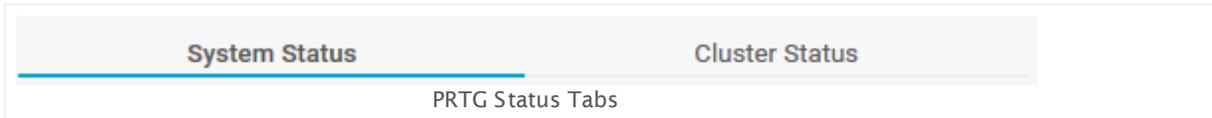
Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

 For how to set a cluster node into **Maintenance Mode**, see [PRTG Status—Cluster Status](#) .

 The entire setup process for a cluster requires several different steps. For more information and step-by-step guidance, see [Failover Cluster Configuration](#) .

8.12.13 PRTG Status—System Status

To view the status of your PRTG installation, select **Setup | PRTG Status** from main menu. Click on the tabs to change the different settings.



You can view the following aspects of the PRTG status:

- [PRTG Status—System Status](#) 3396
- [PRTG Status—Cluster Status](#) 3412

System Status

Click on the **System Status** tab to view relevant system information. You might need this data for debugging or when you contact our support team. They ask you in some cases to provide PRTG status information to analyze your issues with PRTG. Furthermore, this page shows interesting usage statistics. Use the links at the top of the page for quick access to status information.

SOFTWARE VERSION AND SERVER INFORMATION

PRTG Version	Shows the exact version of the build your PRTG installation is currently running on.
Auto-Update Status	Shows the latest auto-update message available from Software Auto-Update <small>3407</small> . For example, the message will indicate any PRTG updates ready to be installed.  This information is not displayed in PRTG hosted by Paessler.
Operating System	Shows the exact Windows version build and service packs, the number and kind of CPUs, and the computer name, of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.  When running PRTG on virtual systems, not all of the mentioned values may be available.  This information is not displayed in PRTG hosted by Paessler.

SOFTWARE VERSION AND SERVER INFORMATION

Server Time	Shows the date and time of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Server CPU Load	Shows the current CPU load of the system the PRTG core server is installed on. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Username	Shows the username ^[3304] of the PRTG user you're currently logged in as.
Browser	Shows the name and user agent string of the browser you're currently viewing this page with.

LICENSING

License Status	Shows the activation status of this installation of PRTG. Usually, PRTG completes the activation automatically during installation or when you change your license information. Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, see Activate the Product ^[99] .
License Name	Shows the owner of the license ^[96] that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.  You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key ^[96] .
License Key	Shows the license ^[96] key that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.
System ID	The system ID is a fixed value that is automatically assigned to your PRTG installation.
Licensed Edition	Shows the PRTG edition that you use for this installation of PRTG. This determines how many sensors you can use in your monitoring (see below).

LICENSING

Last Update	Shows the date of the last update for this PRTG installation. We recommend that you use the PRTG Auto-Update ^[3407] to get the most out of PRTG.
Maintenance until	Shows the expiration date and the days remaining for your active maintenance contract. You can buy maintenance for each PRTG license. With an active maintenance contract you may download any available updates and use our premium email support.
Number of Sensors	<p>Shows the number of sensors you can use in your monitoring with your current edition of PRTG (see above). If you reach the limit, PRTG will set each new sensor that you add to a Pause status^[195] automatically. To upgrade your license right now, click the Need more sensors? Click here to upgrade! button to visit our web shop.</p> <p>Editions that allow an unlimited number of sensors do not restrict the number of possible sensors by license, so you can create sensors until the performance limit^[26] is reached. This means that you can use about 10,000 sensors per core server (depending on your system's performance, sensor types, and scanning intervals). For details, see section Detailed System Requirements^[26].</p>

SYSTEM STARTUP LOG

Shows the log information created during the last startup of the PRTG core server. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

SYSTEM WARNINGS

If there are any warnings, PRTG will show them here. Usually, you will see "None" system warnings.

CLUSTER STATUS

This box is only visible if you run a PRTG cluster. This section lists all cluster nodes configured in your monitoring.

Node **[Number]** Shows the name of the cluster node as well as the node type (primary/secondary node) and status (current master/failover node). Additionally, all connections from this node to the other cluster nodes are shown, as illustrated on the [PRTG Status—Cluster Status](#) 3412 page.

LOCAL STATUS

This box is only visible if you run a PRTG cluster. This section lists information about the cluster node you're currently logged in to.

Server State Cluster Messages Shows internal summary information about the current node and the communication between the nodes. You might be asked about this by Paessler's technical support staff.

CLUSTER CONNECTIONS

This box is only visible if you run a PRTG cluster. This section lists information about the connections between the different cluster nodes.

State of Local Node Shows Treeversion and size of the Server Volume, both internal system information.

State of Cluster Members For each cluster node, the name and IP address is shown, as well as a state CRC code, the time stamp of the last "keep alive" signal sent, the current size of the buffer, and the remote IP.

Message State of Cluster Members For each cluster node, the name, IP address, and unique identifier is shown, as well as the connection state, and statistic information about the cluster message system that is used for the communication between the different nodes.

CORE SYSTEM MEMORY

Shows machine-oriented information regarding the memory usage of the core server system. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

 See the Knowledge Base for more information: [What do the PRTG core system memory parameters mean?](#)

THREAD INFORMATION

Shows machine-oriented information regarding the threads running on the core server system. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

ACTIVITY HISTORY

The "Activity History" shows how busy PRTG was for you in the past. The graphs indicate the number of activities on the last 365 days. Below the graphs, you see statistics about the past day.

Sensor Scans	Shows how often all sensors ¹³⁵ in this PRTG installation refreshed their data in the past.
Sensor State Changes	Shows how often the Sensor States ¹⁹⁵ changed in the past.
Notifications Sent	Shows how many Notifications ³²¹⁶ PRTG sent out in the past.
Reports Generated	Shows how many Reports ³²⁶² PRTG created in the past.
Page Views	Shows how often pages in the PRTG web interface were opened in the past.
Sensors	Shows how many sensors ¹³⁵ existed in this PRTG installation in the past.
Devices	Shows how many devices ¹³⁵ existed in this PRTG installation in the past.

ACTIVITY HISTORY

Reports	Shows how many Reports  existed in this PRTG installation in the past.
Maps	Shows how many Maps  existed in this PRTG installation in the past.

AUTO-DISCOVERY TASKS

Currently Running	Shows the number of auto-discovery tasks that are currently running. A high number of auto-discovery tasks can negatively influence system performance.
-------------------	---

BACKGROUND TASKS

Historic Data	Shows if PRTG is re-calculating the historic data cache in the background. If so, you will see the tasks to do until done. Usually, this calculation is done after every core server restart.
Toplist Buffer	When using xFlow  or Packet Sniffer  sensors, PRTG stores Toplist data. The data stream received is buffered and written to the data directory of the core system. Depending on the number and size of the data stream as well as the hard disk and system performance of the core system, the buffer size can rise. When reaching a buffer size of 500 , Toplist data is dropped, which can lead to incorrect Toplist values for the sensors.
Similar Sensors Detection	Shows the current status and the selected setting for the analysis depth of the Similar Sensors  analysis.
Recommended Sensors Detection	Shows the current status of the detection engine and the current tasks of the Recommended Sensors Detection  .

DATABASE OBJECTS

Shows statistic information about your monitoring configuration. This information might be necessary when contacting Paessler's technical support staff.

Probes	Shows the total number of probes ³⁵¹ configured.
Groups	Shows the total number of groups ³⁷⁵ in your configuration.
Devices	Shows the total number of devices ⁴⁰² in your configuration.
Sensors	Shows the total number of sensors ⁴²⁸ in your configuration.
Channels	Shows the total number of channels ¹³⁶ in your configuration.
User Groups	Shows the total number of user groups ³³⁸³ in your configuration.
Users	Shows the total number of users ³³⁷⁶ configured.
Notifications	Shows the total number of notifications ³³¹¹ configured.
Schedules	Shows the total number of schedules ³³³⁸ configured.
Maps	Shows the total number of created maps ³²⁷⁸ in your installation.
Libraries	Shows the total number of created libraries ³²³⁵ in your installation.
Reports	Shows the total number of reports ³²⁵² in your installation.
Bitfield/Boolean/ Integer/Range Lookups	Shows the total number of used lookups by lookup type ³⁷⁰⁰ .
Requests/Second	Shows a value calculated from the total number of sensors and the average scanning interval configured. This number indicates how many monitoring requests per second are sent from the probe(s) to the devices in your network. There are no general guidelines what is a "good" value here. This depends on the sensor types used as well as on your system's performance.

SENSORS BY PERFORMANCE IMPACT

Shows all sensor types used in your configuration ordered by performance impact (from very low to very high). If your PRTG system is very slow, you can see which sensors might cause this issue. Please consider the recommended number of sensors in the respective [manual sections](#)⁴²⁸ for sensors with high and very high performance impact.

-  In the list, internal short names are used for sensor types instead of the official designations.

SENSORS BY INTERVAL

Shows all sensor types used in your configuration ordered by scanning interval. Please choose reasonable scanning intervals for sensors that can affect the system performance. See the respective [manual sections](#)⁴²⁸ for sensors for more information.

-  In the list, internal short names are used for sensor types instead of the official designations.

PROBES

This section lists all probes configured in your monitoring. If there are no remote probes configured, only the **Local Probe** or **Hosted Probe** appears in the list, which always runs on the PRTG core server.

-  If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. Remote probes (if any) will only be shown when you are logged in to the primary master node. When logged in to a failover node, the cluster probe running on this node will appear as **Local Probe**.

Probe **[#Number]**
"**[Name]**"

Information about the connection status is shown. If the probe is currently connected, the field shows the source IP address and port number used by the probe. For the **Local Probe**, the IP will always be 127.0.0.1. You will also see information about the date when the last data packet was received from the probe.

If you want to restart a single probe, please open the [Administrative Tools Settings](#)³³⁸⁸.

SYSTEM SETTINGS

Web Server URL	Shows the URL to access the PRTG web interface ^[166] . If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server IPs	Shows all IP addresses the PRTG web server is running at. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Ports	Shows the port the PRTG web server is running at. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.
Web Server Port usage	Shows the number of ports used by the PRTG web server.
Incoming Probe Connection Binding	Shows a combination of the two values below.
Incoming Probe Connection IPs	Shows a list of all IP addresses on which your current PRTG installation listens to incoming remote probe connections. This is the same information as shown in the System Administration—Core & Probes ^[398] settings. 0.0.0.0 means that the core server listens on all local network adapter IPs.
Incoming Probe Connection Port	Shows the port number on which your current PRTG installation listens to incoming remote probe connections. The default port is 23560 .
Probe Allow IPs	Shows all source IP addresses that will be accepted by the core server for incoming remote probe connections. This is the same information as shown in the System Administration—Core & Probes ^[398] settings and can be changed there. any means that all remote probe connections are accepted, regardless of the IP address of the remote probe system.
Probe Deny IPs	Shows all source IP addresses that will be denied by the core server for incoming remote probe connections. This is the same information as shown in the System Administration—Core & Probes ^[398] settings and can be changed there. Denied IPs are superior to allowed IPs. If this field is empty, there are no denied IPs.  PRTG automatically adds the IP address of a remote probe system to this list when you delete a remote probe from your device tree ^[133] .

SYSTEM SETTINGS

DataPath Shows the path where PRTG stores its configuration, monitoring database, etc. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to. In order to change this setting, please open the [PRTG Administration Tool](#) on the system of the PRTG core server (or of the respective cluster node, if applicable).

WEB SERVER ACTIVITY

Shows statistic information about the web server since last startup. All values are reset when the core server is restarted. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

Time Since Startup	Shows the time that has passed since the PRTG web server was started.
Page Views	Shows the total number of page views on this core server.
Geo Maps	Shows the total number of geo maps shown on this core server.
HTTP Requests	Shows the total number of HTTP requests to this core server.
HTTP Requests > 500/1000/5000 ms	Shows for how many (percent) of the HTTP requests above the page delivery took longer than 500, 1,000, or 5,000 milliseconds.
Slow Request Ratio	Shows a calculated number of the HTTP request values above. The lower this number, the faster is your installation's web interface.

SYNCHRONIZATION

The core server holds the configuration of the entire monitoring and deploys it to the probes. This section shows statistic information about the synchronization of the core server with the local probe and all connected remote probes (if any), since last startup of the core server. All values shown here are reset when the core server is restarted. If you run a PRTG cluster, this will show information for the system of the cluster node you're currently logged in to.

SYNCHRONIZATION

- ❗ Only when logged in to the primary master node, you will see synchronization data for remote probe connections.

Last Synchronization with a Probe	Shows the time stamp of the last probe synchronization, and if there is still something to do.
Probe/Core Message Count	Shows the total number of messages sent between core and probe(s), as well as a calculated message speed value.
Raw Buffer Count	Shows the number of raw buffers and a corresponding status indicator.
Configuration Requests Sent	Shows the total number of configuration requests and the requests that still have to be sent.
Configuration Requests Deleted	Internal debug information. Usually, this value will be 0.
Configuration Requests With Response	Internal debug information. Usually, this value will be 0.

More

Paessler Website: System Requirements for PRTG Network Monitor—Recommended Setup for Most PRTG Users

- <https://www.paessler.com/prtg/requirements>

Knowledge Base: How can I speed up PRTG—especially for large installations?

- <https://kb.paessler.com/en/topic/2733>

Knowledge Base: What do the PRTG core system parameters mean?

- <https://kb.paessler.com/en/topic/71671>

8.12.14 PRTG Status—Auto-Update

Whenever a new version of the software is available from the Paessler website, PRTG will download the setup file automatically if a direct internet connection is available. The **PRTG System Administrator** user will then receive a [ToDo ticket](#)^[230] with instructions to initiate the update installation.

For customers using a [Freeware or Trial Edition](#)^[21], automatic software updates are available at any time. Customers using a [Commercial Edition](#)^[21] need to have an active maintenance contract to receive updates.

 This option is not available in PRTG hosted by Paessler.

Status

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

To view the auto-update page of your PRTG installation, select **Set up | Auto-Update** from main menu. On the **Status** tab, you can download and perform updates.

Using Auto-Update

If there is a new version available, you will see detailed information about the available version. Please read these notes carefully! You find a summary of current and past release notes below the update section. For detailed release notes, click **PRTG Release Notes and Version History**, which will redirect you to the [version history page on paessler.com](#).

To install the latest available version, click **Install Update [version number]**. PRTG will ask you to confirm installation and license—and that's it!

 Downloaded software versions are automatically saved in the [PRTG program directory](#)^[3734] in the **\download** subfolder. The **prtg.zip** that contains all necessary files is also cached in this folder.

Part 8: Ajax Web Interface—Advanced Procedures | 12 Setup 14 PRTG Status—Auto-Update

Here you can automatically update your PRTG installation.

- If you are using the freeware or trial edition you can always update to the latest version for free
- If you are using a commercial edition your license key must be covered by a valid maintenance contract in order to download updates.
- You can always prolong your maintenance at <https://shop.paessler.com>

You can deactivate automatic downloading in the [Settings](#) tab.

Update Status For PRTG Network Monitor

Remaining Maintenance Days	4704 (4/29/2030)
Latest Message from Auto-Update	[6/12/2017 3:50:05 PM] Downloaded version (17.2.32.2190) is not newer than your current version (17.2.32.2194).
Currently Installed Version	17.2.32.2194+
Currently Selected Release Channel	Canary Select Other Release Channel
Latest Version Available from Paessler	17.2.32.2196 NEW! Check For Latest Update and Download
Latest Downloaded Version	

Automatic Software Update Page

Manually Install an Interim Update

Not all available updates from Paessler will be pushed to all customers, but they are still available from the website. Sometimes Paessler Support may ask you to update to the latest version.

In this case please click the **Check For Latest Update and Download** button. PRTG will then connect to the Paessler servers and download the setup file, regardless of the status of the update-check. Then **Install Update [version number]**.

 To use this function, a direct internet connection is necessary on the computer running the PRTG core server.

Select Other Release Channel

PRTG is available in three different release channels.

 For details about continuous rollout and release channels, see the Paessler Blog: [Version 12 of PRTG will introduce "Continuous Rollout"](#)

To change the release channel you receive updates from, please open the auto-update [Settings](#)³⁴⁰⁹ tab and choose the desired release channel in the **Release Channel** section.

Log

Click the **Log** tab to show log information about the update status of PRTG, newest first. In the [table list](#)²³⁷ appearing, you can filter the items by using the [respective options](#)²³⁷.

 For more information, see the [Logs](#)²²⁸ section.

Settings

Click the **Settings** tab to configure the PRTG **Software Auto-Update**.

SOFTWARE AUTO-UPDATE

When a New Version is Available	<p>Define what to do when there are software updates available. Choose between:</p> <ul style="list-style-type: none"> ▪ Automatically download and install the latest version: PRTG automatically downloads and installs any new version as soon as PRTG detects that there is a newer version available (PRTG checks this once per day). <ul style="list-style-type: none">  The installation of a new version will restart the PRTG Windows services and may also include a server restart. ▪ Automatically download the latest version and alert the admin: PRTG automatically downloads any new version as soon as PRTG detects that there is a newer version available (PRTG checks this once per day). After successful download, PRTG will create a ToDo ticket²³⁰ for the PRTG System Administrator user. ▪ Alert the admin only: When PRTG detects that there is a newer version available, it will not download updates automatically, but create a ToDo ticket²³⁰ only. You can still download updates manually on the Auto-Update³⁴⁰⁸ page.
Installation Time	If you select the automatic installation option above, choose the desired time for installation of updates from the dropdown menu.
Release Channel	<p>PRTG updates are delivered in different release channels. You can choose between maximum stability, or most early access to new features. Choose between:</p> <ul style="list-style-type: none"> ▪ Stable: Updated about once per month (most conservative option, recommended): These are our best tested versions. Choose this channel for live environments you have to depend on! ▪ Preview: Updated about once per week: Versions in this channel are already thoroughly tested in our labs, but may still contain limitations in certain monitoring configurations. Choose this channel if you are willing to take a little risk for the benefit of getting new features and bug fixes a little earlier. We strongly recommend to not use those versions in live environments you have to depend on!

SOFTWARE AUTO-UPDATE

- **Canary: Updated daily (testing only, should not be used on live systems):** Updated every night. Use with CAUTION! Software versions in this channel are not tested yet, might contain severe bugs, and are provided for testing purposes only. We strongly recommend to **not** use those versions in live environments you have to depend on!

 For details about continuous rollout and release channels, see the Paessler Blog: [Version 12 of PRTG will introduce "Continuous Rollout"](#)

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Notes

There are a few things we ask you to consider regarding automatic software updates:

- In order for auto-update to work, the machine running the PRTG core server needs direct internet access. If a proxy connection is needed, please configure it in the [System Administration—Core & Probes](#)³³⁶⁸ settings.
 For details about the update servers, see this Knowledge Base article: [Which servers does PRTG connect to for Software Auto-Update and for Activation?](#)
- During installation the core server may be restarted without notice.
- PRTG updates existing remote probes automatically, causing short downtimes in monitoring of remote locations. In rare cases a manual update of remote probes is required after you update the core server. In these cases you will be notified in the device tree, and monitoring of remote locations will be interrupted until you perform the [manual update](#)¹⁰¹¹ on the system(s) running the remote probe(s). If a server with a probe uses several network connections with different IP addresses, ensure these addresses are included in the [list of allowed IPs](#)³³⁶⁹. Otherwise the remote probe on this machine might be disconnected after an update.
- In a cluster installation the update needs to be installed on one node only. The new version will then be deployed to all other cluster nodes automatically (causing a short downtime for the monitoring on the cluster nodes, one after another).
- If you run several individual PRTG core servers that are not in a cluster, for example, in combination with the [Enterprise Console](#)³⁴³¹, an update has to be initiated and confirmed for each single core server.
- You can disable automatic downloading on the [Auto-Update Settings](#)³⁴⁰⁹ tab. Updates will then only be downloaded on request, when you click the **Check For Latest Update and Download** button.
- PRTG does not start auto-update downloads if there is less than 500 MB disk space available on the core server system. If this is the case, you can check this on the [Log](#)³⁴⁰⁸ tab.

- Virus scanners can potentially cause issues when downloading or installing software updates. To avoid such issues, we recommend that you make the appropriate exclusions for the [PRTG program directory](#)³⁷³⁴.

More

Knowledge Base: Which servers does PRTG connect to for Software Auto-Update and for Activation?

- <https://kb.paessler.com/en/topic/32513>

Knowledge Base: Which information does PRTG send back to Paessler?

- <https://kb.paessler.com/en/topic/28103>

Knowledge Base: How and where does PRTG store its data?

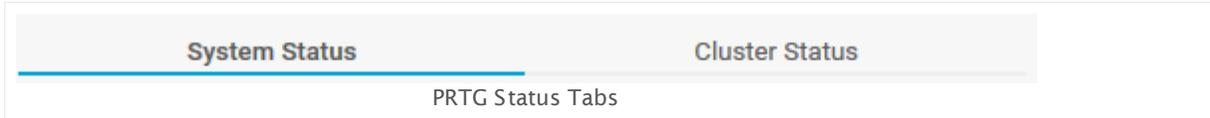
- <https://kb.paessler.com/en/topic/463>

Paessler Blog: Version 12 of PRTG will introduce "Continuous Rollout"

- <https://www.paessler.com/blog/2012/04/25/news/prtg-12-introduces-continuous-rollout>

8.12.15 PRTG Status—Cluster Status

To view the status of your PRTG installation, select **Setup | PRTG Status** from main menu. Click on the tabs to change the different settings.



You can view the following aspects of the PRTG status:

- [PRTG Status—System Status](#) ³³⁸⁶
- [PRTG Status—Cluster Status](#) ³⁴¹²

Cluster Status

Click the **Cluster Status** tab to view all nodes connected to the cluster. This tab is only available if you run PRTG in [cluster mode](#) ¹³⁰. The following information is available:

- **Cluster Status** with all connected nodes as table and graphic
- **Cluster Log** with all log entries for cluster connections

The screenshot displays the 'Cluster Status' view in the PRTG interface. It features two main sections: 'Cluster Status' and 'Cluster Log'.

Cluster Status Section:

- Node 1: PRTG Network Monitor (10.0.10.34)**
 - Primary Node (Current Master)
 - Action: Start Maintenance Mode
 - Connection To: Node 10.0.10.35, IP: 10.0.10.35, State: Connected
- Node 2: Node 10.0.10.35**
 - Secondary Node (Failover Node, Version: 50186)
 - Action: Start Maintenance Mode
 - Connection To: PRTG Network Monitor (10.0.10.34), IP: 10.0.10.34, State: Connected

A diagram above the nodes shows a 'Failover Node' (Node 10.0.10.35) and a 'Current Master' (PRTG Network Monitor (10.0.10.34)) connected by a bidirectional arrow.

Cluster Log Section:

Select Range: Show filter Date Range: 2017-06-05 00:00 - 2017-06-13 00:00 Items: > 50

Date Time	Parent	Type	Object	Status	Message	Cluster Node
6/9/2017 2:41:30 PM	None	Probe	Cluster Probe	Connection connected	Cluster: Connected to node CF0...	PRTG Network Monitor (10.0...
6/9/2017 2:41:30 PM	None	Probe	Cluster Probe	Cluster	Node 1 Connection 1 (10.0.10.3...	PRTG Network Monitor (10.0...
6/9/2017 2:41:30 PM	None	Probe	Cluster Probe	Cluster	Node 1 Connection 1 (10.0.10.3...	PRTG Network Monitor (10.0...
6/9/2017 2:41:25 PM	None	Probe	Cluster Probe	Connection disconnected	Cluster: Lost connection to nod...	PRTG Network Monitor (10.0...
6/9/2017 2:41:20 PM	None	Probe	Cluster Probe	Connection connected	Cluster: Connected to node 85F...	Node 10.0.10.35
6/9/2017 2:41:20 PM	None	Probe	Cluster Probe	Cluster	Node 2 Connection 1 (10.0.10.3...	Node 10.0.10.35
6/9/2017 2:36:40 PM	None	Probe	Cluster Probe	Cluster	Cluster: Sending software upda...	PRTG Network Monitor (10.0...
6/9/2017 2:36:40 PM	None	Probe	Cluster Probe	Cluster	Cluster: Access denied for node...	PRTG Network Monitor (10.0...
6/9/2017 2:36:36 PM	None	Probe	Cluster Probe	Connection connected	Cluster: Connected to node CF0...	PRTG Network Monitor (10.0...
6/9/2017 2:36:36 PM	None	Probe	Cluster Probe	Cluster	Node 1 Connection 1 (10.0.10.3...	PRTG Network Monitor (10.0...
6/9/2017 2:36:36 PM	None	Probe	Cluster Probe	Cluster	Node 1 Connection 1 (10.0.10.3...	PRTG Network Monitor (10.0...

Example of a PRTG Cluster Status View

Click the **Start Maintenance Mode** link to put a cluster node in maintenance mode. A node in this mode is still connected to the cluster, but its monitoring results are discarded until you click the **Stop Maintenance Mode** link. You can use this functionality to explicitly exclude a node from monitoring if you know that the monitoring values will not be accurate, for example, because you reconfigure the failover server. During maintenance, a cluster node is displayed with a transparent color in the overview graphic.

 On this page, you will not see if your [remote probes are connected to failover nodes](#)³⁷²³. Please connect to your failover nodes and check explicitly if remote probes are connected (for example, in the device tree of the PRTG web interface on a cluster node).

 For more information about cluster settings, see section [System Administration—Cluster](#)³³⁹⁴.

 This feature is not available in PRTG hosted by Paessler.

8.12.16 PRTG Status—Licensing Status and Settings

To view information about the license of your PRTG installation and to enter your license key, select **Setup | License** from the main menu.

 This option is not available in PRTG hosted by Paessler.



You can view the following aspects of your PRTG license:

- [Your License—Status](#)  ³⁴¹⁴
- [Your License—Log](#)  ³⁴¹⁵
- [Update Your License](#)  ³⁴¹⁶

 If you use PRTG on premises and open the system administration page from another administration page, PRTG will ask you to enter your credentials again for security reasons if 15 minutes (900 seconds) have passed since your last credential-based login. A dialog box will appear. Enter your **Login Name** and **Password** for PRTG in the corresponding fields and confirm to continue.

 This documentation refers to the **PRTG System Administrator** user accessing the PRTG web interface on a master node. If you use other user accounts, interfaces, or nodes, you might not see all of the options in the way described here. If you use a cluster installation, note that failover nodes are read-only by default.

Status

Click the **Status** tab to view information about your license.

LICENSING	
License Status	Shows the activation status of this installation of PRTG. Usually, PRTG completes the activation automatically during installation or when you change your license information. Only if PRTG cannot connect directly to the internet, a manual activation is necessary. For details, see Activate the Product  ⁹⁹¹ .
License Name	Shows the owner of the license  ⁹⁶¹ that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.

LICENSING

 You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you [change your license key](#)^[96].

License Key	Shows the license ^[96] key that you use for this installation of PRTG. License Name, license key, and system ID together build your license information.
System ID	The system ID is a fixed value that is automatically assigned to your PRTG installation.
Licensed Edition	Shows the PRTG edition that you use for this installation of PRTG. This determines how many sensors you can use in your monitoring (see below).
Last Update	Shows the date of the last update for this PRTG installation. We recommend that you use the PRTG Auto-Update ^[3407] to get the most out of PRTG.
Maintenance until	Shows the expiration date and the days remaining for your active maintenance contract. You can buy maintenance for each PRTG license. With an active maintenance contract you may download any available updates and use our premium email support.
Number of Sensors	Shows the number of sensors you can use in your monitoring with your current edition of PRTG (see above). If you reach the limit, PRTG will set each new sensor that you add to a Pause status ^[195] automatically. To upgrade your license right now, click the Need more sensors? Click here to upgrade! button to visit our web shop. Editions that allow an unlimited number of sensors do not restrict the number of possible sensors by license, so you can create sensors until the performance limit ^[26] is reached. This means that you can use about 10,000 sensors per core server (depending on your system's performance, sensor types, and scanning intervals). For details, see section Detailed System Requirements ^[26] .

Log

Click the **Log** tab to show a [table list](#)^[237] of all system log entries with all messages and status changes regarding your license.

Change and Update License Information

Use the buttons to edit your license or refresh your maintenance information.

- **Change License Key:** If you want to use another license for this PRTG installation, for example, after an license upgrade, click this button to change your license information. See [below](#) ³⁴¹⁶ for more details.
- **Refresh Information:** If you have renewed your maintenance and the licensing information above does not show the new maintenance period yet, click this button to manually refresh your maintenance information. An automatic refresh of the maintenance information may take several days. See [below](#) ³⁴¹⁶ for more details.
- **Deactivate this License:** If you want to use the license of the current PRTG installation on another computer, click this button to deactivate the license. This is necessary, for example, when you move PRTG to another computer, because a PRTG license can be active on only one computer at the same time. Once you have deactivated the license, the PRTG installation on this computer will revert to the [Freeware Edition](#) ²¹ after a grace period of 30 days.

 See also section [Activate the Product](#) ⁹⁹.

Update Your License Information

Click **Change License Key** or **Refresh Information** on the **PRTG License** page to update your license. Provide the necessary information and click **Update License** to complete the activation of your license.

 If you have any issues with license activation or update, please click the **Contact Support** button to contact us directly via the [Paessler Service Center](#) in our shop (internet access required).

STEP 1: CHOOSE ACTIVATION TYPE

Activation Type	<p>Define how you want to validate and activate your license. Choose between:</p> <ul style="list-style-type: none"> ▪ Automatic (online activation with optional HTTP proxy): PRTG will connect to the activation server and validate your license. The license will be activated automatically. For automatic activation, internet access is necessary from the the computer running this PRTG installation. ▪ Manual (offline activation): Choose manual activation if the PRTG server has no access to the internet and cannot connect to activation.paessler.com.  This is the default selection if the PRTG server is offline.
-----------------	--

STEP 2: VERIFY YOUR PRTG LICENSE

License Name	<p>Enter the License Name that you have received from us, the Paessler AG. It must exactly match. To avoid typing errors, please copy and paste the License Name.</p> <p> You will find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name for which you will be asked while installing PRTG or when you change your license key^[96].</p>
License Key	<p>Enter the license key you have received from us, the Paessler AG. To avoid typing errors, please copy and paste the License Key. It must exactly match your license key.</p>
System ID	<p>This field shows the system ID, a fixed value assigned to your PRTG installation. This setting is shown for your information only and cannot be changed here.</p>

For offline activation, click **Save to File** to write your license information into a text file.

STEP 3: ACTIVATE YOUR PRTG

If you select the automatic activation type, you can now update your license. Define if you need an HTTP proxy for the HTTPS connection to the activation server and click **Update License**.

PROXY CONFIGURATION

 This option is not available in PRTG hosted by Paessler.

Use Proxy Server	<p>We recommend that you use PRTG with a direct internet connection. However, if you need to use a proxy, you can configure the relevant settings here. Choose between:</p> <ul style="list-style-type: none">▪ No, use direct connection to the internet (default): Do not use a proxy. Use this setting if there is a direct internet connection available to the server running the PRTG core server.▪ Yes, in our network a proxy is mandatory: Define proxy settings below.
------------------	---

PROXY CONFIGURATION

 Proxy settings are valid for [Auto-Update](#)³⁴⁰⁷, [Activate the Product](#)⁹⁹, obtaining [Geo Maps](#)³²¹¹ tiles, and for sending out HTTP, push, and SMS text message [Notifications](#)³³¹⁶.

Proxy Server	This setting is only visible if proxy usage is enabled above. Enter the address of the proxy server that you use for outbound connections. Please enter a valid address.
Port	This setting is only visible if proxy usage is enabled above. Enter the port number of the proxy server that you use for outbound connections. Please enter an integer value.
Use Proxy Credentials	This setting is only visible if proxy usage is enabled above. Determine whether the proxy server needs credentials or not. Choose between: <ul style="list-style-type: none"> ▪ No, there are no credentials necessary: Do not use credentials for proxy connections. ▪ Yes, the proxy server requires credentials: Define credentials (username and password) below.
User	This setting is only visible if proxy credentials are enabled above. Enter a username for proxy authentication. Please enter a string.
Password	This setting is only visible if proxy credentials are enabled above. Enter a password for proxy authentication. Please enter a string.

STEP 3: REQUEST ACTIVATION DATA

If you select the manual activation type, you have to request your activation data on <https://www.paessler.com/activation> using your license information. Open the activation page from a computer that can connect to <https://www.paessler.com> and provide your license information.

Generate the key file for your license and provide this data below.

STEP 4: PROVIDE ACTIVATION DATA

This step is only necessary if you do an offline activation.

- Copy the content of the key file that you have generated on <https://www.paessler.com/activation>.
- Paste it into the **Activation Data** field. Alternatively, click **Load from File** if you have saved the key file with your activation data.
- Click **Update License** to complete the activation of your license.

8.12.17 Optional Downloads and Tools

To see optional downloads, select **Setup | Downloads and Tools** from the main menu. Click a tab to switch between different options.



There are the following downloads available:

- [Client Apps for Mobile Devices](#) 
- [Client App for Windows \(Enterprise Console\)](#) 
- [Remote Probe Installer](#) 
- [PRTG Tools](#) 

Client Apps for Mobile Devices

To monitor your network while on the go, use our free apps for smartphones and tablets. They run on iOS and Android.

 For more information on **PRTG for iOS** and **PRTG for Android**, see the Paessler Website: [Mobile Network Monitoring with PRTG—Mobile Apps for Smartphones and Tablets](#)

Client App for Windows (Enterprise Console)

Download the Windows Graphical User Interface (GUI) **Enterprise Console** to the current system. If you use the Enterprise Console, you can access the PRTG on premises web interface with a native Windows application. The version of the Enterprise Console must match the version of your PRTG server.

 For more information, see [Install the Enterprise Console](#) 

 This feature is not available in PRTG hosted by Paessler.

Remote Probe Installer

With remote probes you can extend your monitoring to distributed networks that are not directly reachable from your PRTG core installation. The version of the remote probe installer must match your version of PRTG, so it is a good idea to download it from here.

 For more information, see section [Install a PRTG Remote Probe](#) 

PRTG Tools

You can use several freeware tools directly from the Paessler labs that help you to manage your network and to diagnose and test network monitoring issues. Open the **PRTG Tools** tab and click the **More Information and Download** button to navigate to our freeware tools webpage. There you can find a collection of various tools for PRTG Network Monitor.

 Find all tools on the Paessler Website: [Freeware Network Tools](https://www.paessler.com/tools)

More

Paessler Website: Mobile Network Monitoring with PRTG—Mobile Apps for Smartphones and Tablets

- <https://www.paessler.com/apps>

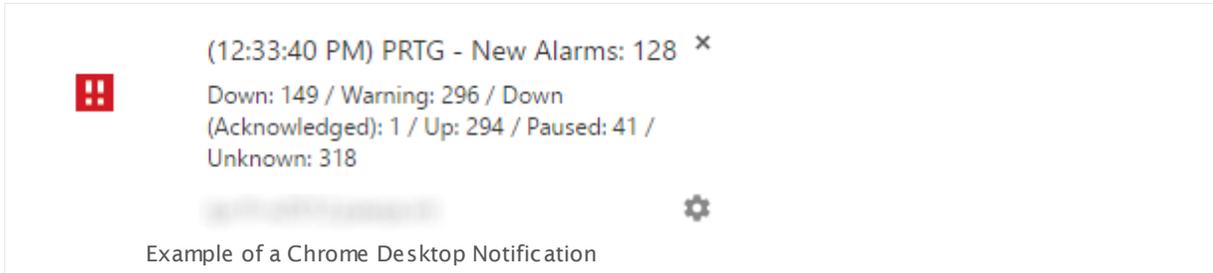
Paessler Website: Freeware Network Tools

- <https://www.paessler.com/tools>

8.12.18 Desktop Notifications

While you are logged in to the PRTG web interface with your Google Chrome or Firefox browser, PRTG can show notifications on your desktop whenever there are new alarms in your monitoring.

PRTG will show desktop notifications (by default, in the lower-right corner of your desktop) whenever there are new alarms after a page refresh in the PRTG web interface. The notification displays the number of new alarms and the current number of each sensor status.



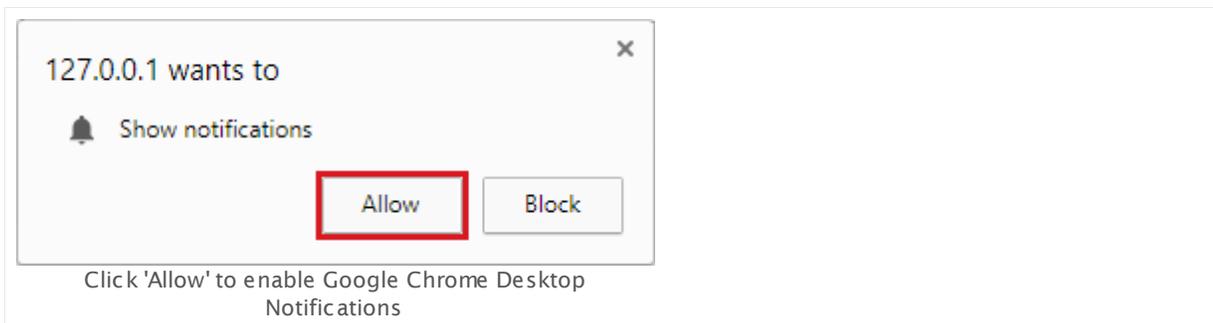
i Desktop notifications are not available for Internet Explorer.

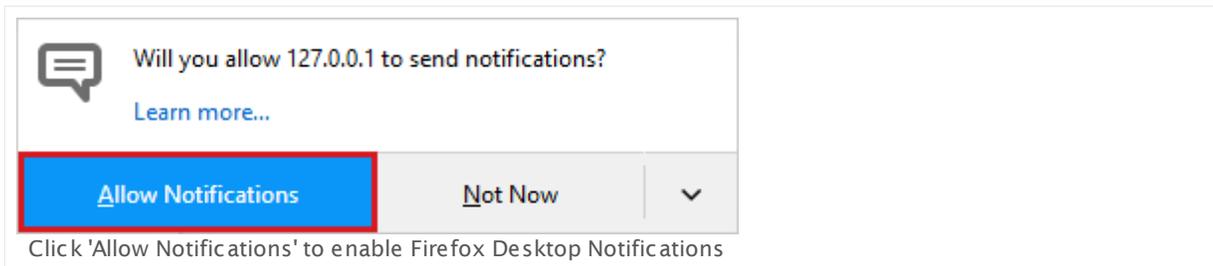
Desktop Notifications Settings

When you log in to the PRTG web interface, a message appears, asking you to allow desktop notifications. You have to initially allow the notifications for each installation/profile of Firefox or Google Chrome.

i Desktop Notifications in Google Chrome are not available for HTTP connections. See section [System Administration—User Interface](#) for more information.

- In Google Chrome, click **Allow** to add the URL of the PRTG web interface to the allowed sites.
- In Firefox, click **Allow Notifications** to add the URL of the web interface to the allowed sites.





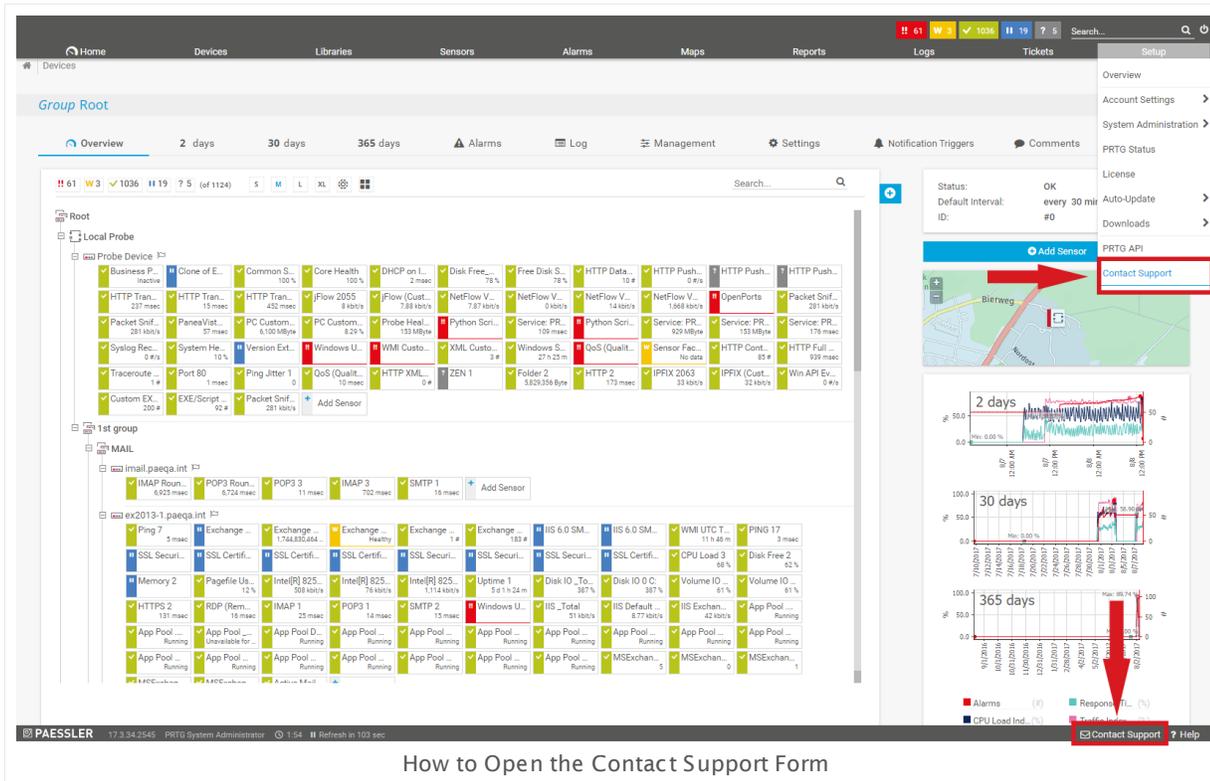
Disabling or Re-Enabling Desktop Notifications

To disallow or re-allow desktop notifications for the PRTG web interface, edit your browser options:

- In **Google Chrome**: Click the **View site information** symbol in the address bar of the browser. You can block or re-allow notifications for the current URL in section **Notifications**.
- In **Firefox**: Click the **Show site information** symbol in the address bar of the browser. You can block or re-allow notifications for the current URL in section **Permissions**.

8.12.19 Support—Contact Support

For technical issues, please use the **Contact Paessler Support / Send Your Feedback to Paessler** form in PRTG. To open the form, select **Setup | Contact Support** from the main menu. You can also open the form via **Contact Support** in the footer on every page in PRTG.



How to Open the Contact Support Form

On the one hand, you can use this form to give us **feedback**. Help improve PRTG by providing criticism, praise, bug reports, and feature requests. Any comments are welcome! Your feedback will be handled directly by the Paessler Support Team.

On the other hand, you can use this form to ask for support regarding technical issues. To make the support contact more comfortable, PRTG can automatically attach a screenshot in combination with a **Support Bundle** that contains several selected PRTG logfile and status files. This information really helps our support team to analyze any issues you may have with PRTG. Please also consider the suggested links to articles regarding the scope of your issue.

Premium Email Support

We offer our support directly from our headquarters in Nuremberg, Germany, working closely with our development department to guarantee the fastest and most constructive assistance possible. As we have to analyze a lot of data over the course of a support case, like logfile and screenshots, we use email as our primary support mechanism. Our office is staffed Monday to Friday from 7 a.m. until 10 p.m. (UTC+1), so you will receive an answer within 24 hours on business days. Depending on the complexity of the case, we may need to ask for remote access to your system, or to schedule a remote desktop session.

Support Ticket System

Customers with valid maintenance can open support tickets. Please use the **Contact Support** form of your PRTG installation for technical questions to get the best possible help from our experts. If you have trouble using this form, you can fill out the [support ticket form on our webpage](#).

Updates and Your License Key

Are you looking for updates or your license key? Log in to our [service center](#).

Language

Please write us in English or German language.

Single Topics

Please open a new ticket for each new topic.

Security Reports

If you are a user of PRTG or any other of our services and would like to file a security report, please send an email to security@paessler.com. Please always include a detailed technical summary in your email. If you wish to send us an encrypted email, please use the public key on this page <https://www.paessler.com/support>.

Network Planning

Do you need assistance for your network setup or detailed installation planning? Our partners are happy to help. Please [contact a partner near you](#).

Freeware Users

Do you use our Freeware? We try to answer your questions in a timely manner, but if we are busy, paying customers come first. You may find a prompt answer in our [Knowledge Base](#).

Feature Requests

You have requests or suggestions that could improve PRTG Network Monitor? Our [Support Team](#) is happy to hear your ideas! Read more in our Knowledge Base on [how we handle your feedback](#).

 PRTG securely transmits your feedback or support question including the support bundle to Paessler via the PRTG Cloud. Please make sure your PRTG server has access to the internet and can reach the URL <https://api.prtgcloud.com:443>

Contact Paessler Support / Send Your Feedback to Paessler
✕

Ask a Question or Give Us Your Feedback

Your Ticket ID PAExxxx
(If You Have One)

Your Email Address

john.q.public@company.com

Scope of Your Question

PRTG configuration and usage

PRTG clients (Enterprise Console and mobile apps)

Technical issues (performance, webserver, sensors, probes, cluster)

Critical issue (large parts of my monitoring do not work)

Other (including feedback and feature requests)

Tech Support resources that may be helpful for you:

- Help with installation, licensing, and setup
- Information about data storage/backup/migration and updating PRTG
- Working with user accounts and user rights
- Installing an SSL certificate for the PRTG web server
- Configuring failover clustering

Emotional State

OK ▼

Describe Your Question in One Sentence

Cancel
Submit

Contact the Paessler Support or Send Feedback

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the contact form:

- **Your Ticket ID PAExxx:** If you have already opened a new ticket (directly via email to support@paessler.com, via the [Knowledge Base](#), or via the [support form on paessler.com](https://support.paessler.com)), enter its ID here. You can find it in your confirmation email regarding the request we received. You can provide the ID with "PAE" in front or just the number. If you leave this field empty, you will create a new ticket when you submit this form.
- **Your Email Address:** Enter your email address here. You can provide any of your addresses; however, the recommended and default address is the email address of your PRTG account to be able to associate you with your license.
- **Scope of Your Question:** Select a topic regarding your issue and consider the proposed links.
- **Emotional State:** If you want to, you can indicate your current feelings about PRTG.
- **Describe Your Question in One Sentence:** Provide short information with max. 60 characters to indicate the topic of your issue.
- **Do You Have Any Further Comments?:** Leave your comments here. They can be feedback or support questions. If you have a support question, please describe your issue with as many details as possible!

Attach a Screenshot and/or Support Bundle

To provide the most helpful information possible, you can attach a screenshot of the current page and a support bundle with useful analytical data about your PRTG installation.

In section **Screenshot**, choose between:

- **Do not attach screenshot:** Send the ticket without a screenshot.
 - ⓘ We recommend that you attach a screenshot of the affected PRTG webpage so that we can understand your request more easily.
- **Create and attach screenshot (recommended):** Create a screenshot of the currently displayed page in PRTG to send it with your ticket. You can see a preview below the screenshot section.
 - ⓘ If you encounter issues on a specific page in PRTG, open the contact support form on this page to get a screenshot of it. This is not possible on error pages, which are not meaningful enough for our support team to solve your issue.

In the section **Support Bundle**, you can choose between several packages that differ in coverage of information:

- **Attach Base Pack with logfiles (recommended):** Contains logfiles of your PRTG installation and the following information:
 - System status
 - Lists of sensors regarding their current states
 - Core state data
 - Probe Health sensor data
 - Current log entries

- **Attach Base Pack with log files and PRTG configuration file:** Additionally contains the configuration file.
 - ⚠ Send this package only if our support team told you so! Encrypted passwords in the config.dat file and passwords that your browser masks while you enter them on settings pages will be removed before PRTG sends this package to Paessler Support.
- **Do not attach a Support Bundle:** The ticket will not contain files. Choose this option only when sending feedback.

Click the **Submit** button to send your request directly to our technical support team, or click **Cancel** to return to the page where you opened the contact form. Usually, you will receive an answer from our support team within one or two business days, no matter whether you provide feedback or you have a question.

- ⚠ If you have questions or feedback regarding your license purchase, upgrade, or maintenance extension, please [contact our customer service](#)¹⁷⁸.

More

Knowledge Base: How does Paessler handle user feedback and feature requests?

- <https://kb.paessler.com/en/topic/33873>

Part 9

Enterprise Console

9 Enterprise Console

The Enterprise Console (in old PRTG versions called "Windows GUI") is one alternative [interface](#) ^[125] that you can use to connect to the PRTG core server to configure your setup, view monitoring results, and keep an eye on your network. It is a native Windows application for fast access to data and monitoring management.

The Enterprise Console (EC) provides extended pop-up window functionalities, as well as a seamless link to the [Ajax web interface](#) ^[166] where you can change your monitoring configuration and access further functionalities such as [reporting](#) ^[3454], [maps](#) ^[3452], [system setup](#) ^[3463], [tickets](#) ^[3458], and [libraries](#) ^[3448]. The EC shows most of the functions with an embedded webkit browser, for a few options the EC opens an external browser window (using your default browser).

Remarks

-  There are some known issues with the Enterprise Console. Because we are currently developing a new PRTG desktop client, we will not patch the following issues anymore.
 - The Enterprise Console runs under all [supported Windows versions](#) ^[26], but it is not fully compatible with Windows 10. Running the EC on Windows 10 results in several issues, so please use another operating system.
 - The Enterprise Console does not support [System Information](#) ^[222] and does not show this tab on devices. Please use the PRTG web interface to access system information of a device.
 - Starting the auto-discovery from the [context menu](#) ^[3480] via **Auto Discovery | Run Auto-Discovery** does not work. Please use the PRTG web interface to instantly run an [auto-discovery](#) ^[3407].
-  PRTG hosted by Paessler does not support connections from the Enterprise Console. If you want to use it, please connect the Enterprise Console to a PRTG on premises instance.

Access Several Core Servers in One Console

As an additional functionality, you can configure access to several PRTG core servers in the Enterprise Console. It can show data of all your independent core server installations at a glance (for example, the [device tree](#) ^[3439] and [alarms list](#) ^[3450]), so you can manage your monitoring centrally, also when it is spread across different servers.

Getting Started

Every installation of PRTG Network Monitor includes the Enterprise Console and installs it automatically on the computer running the PRTG core server. If you want to use the Enterprise Console on another computer, please [download](#) ^[3420] and install it there. For details, see the [Install the Enterprise Console](#) ^[113] section.

 The Enterprise Console is mainly designed to review and manage an existing installation of PRTG that you have already set up. If you just start monitoring, we recommend that you first run through the [Smart Setup](#)^[521] in the [PRTG web interface](#)^[166] and add your network devices there.

 For detailed instructions, see section [Quick Start Guide](#)^[46]. Once finished, you can seamlessly switch to the Enterprise Console.

Requirements for Connections to PRTG Web Server(s)

To show monitoring data of your PRTG setup, the Enterprise Console must be able to establish a connection to your PRTG web server(s). For this purpose, please ensure the following.

- The following server settings in the Enterprise Console have to match the following settings in the [PRTG Administration Tool](#)^[3561].
 See section [PRTG Servers](#)^[3463] for details.

ENTERPRISE CONSOLE SERVER SETTINGS	PRTG ADMINISTRATOR SETTINGS
Server IP / DNS name	IP address for PRTG's Web Server on the Web Server tab
Port	<p>TCP Port for PRTG's Web Server on the Web Server tab</p> <p> PRTG switches to port 8080 as a fallback after a restart when port 80 is already used, and to port 8443 if port 443 is not available. PRTG keeps the SSL connection in this case. If this port is also not available, PRTG tries from port 32000 on until it finds an available port. Because the EC cannot recognize these ports (8080, 8443, 32000+) automatically, enter the currently used port manually here in the Port setting. If you do not get a connection to the PRTG web server, check the currently used port in the Web Server settings under System Administration—User Interface^[3346] in the PRTG web interface.</p>
Login Name	Login Name on the Administrator tab
Password	Password on the Administrator tab

- No local software firewall blocks the connection.
- No local virus protection program blocks the connection.
- The specified port is not used by another application.
- No (hardware) firewall blocks the connection when connecting through a network (LAN or WAN).

- The software versions of the Enterprise Console and the PRTG web server have to match at least in the third number (for example, [EC version](#)³⁴³⁷ 15.3.18.3590 can connect to [server version](#)¹⁸¹ 15.3.18.3796).

 For common issues with the Enterprise Console and their solutions, see this Knowledge Base article: [Problems with the Enterprise Console: What can I do?](#)

More

Knowledge Base: Problems with the Enterprise Console: What can I do?

- <https://kb.paessler.com/en/topic/60091>

Enterprise Console—Topics

- [First Start](#)³⁴³³
- [General Layout](#)³⁴³⁴
- [Menu Tabs and Page Content](#)³⁴³⁸
- [PRTG Servers](#)³⁴⁶³
- [Options](#)³⁴⁶⁶
- [Windows Menu Structure](#)³⁴⁷²
- [Context Menus](#)³⁴⁸⁰
- [Shortcuts Overview](#)³⁴⁸¹

Related Topics

- [Ajax Web Interface—Basic Procedures](#)¹⁶⁶
- [Ajax Web Interface—Device and Sensor Setup](#)²⁸⁰
- [Ajax Web Interface—Advanced Procedures](#)³¹⁸⁴

9.1 First Start

This section helps you to start the Enterprise Console for the first time.

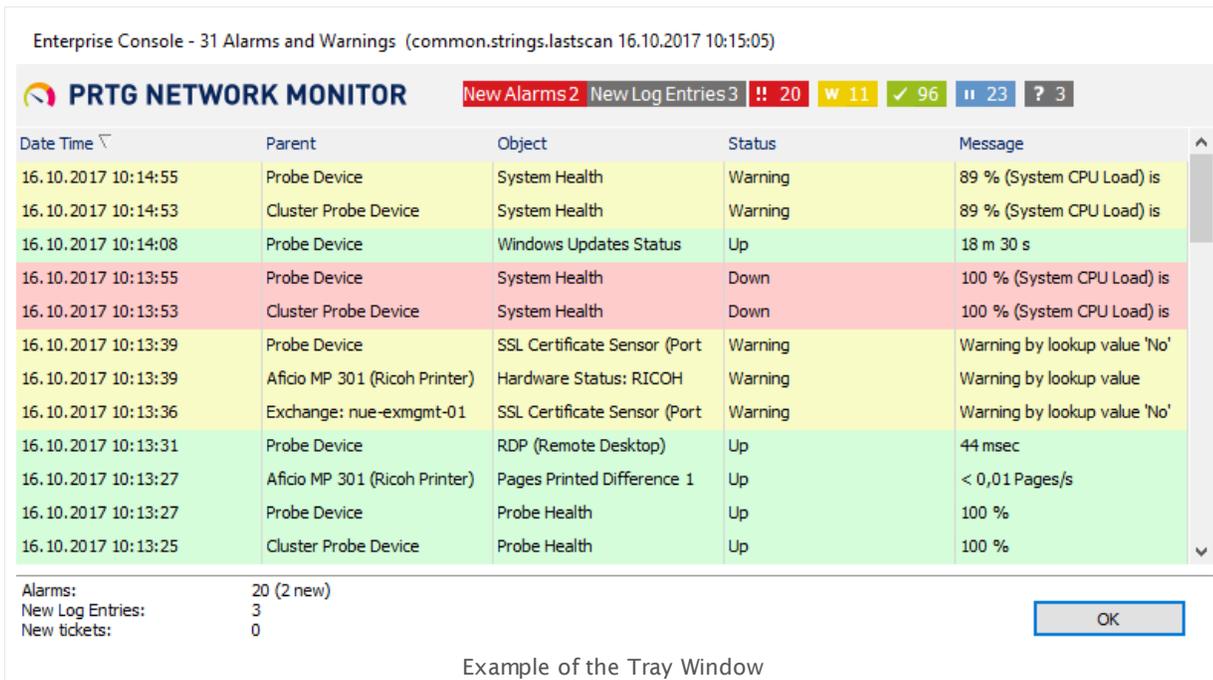
Open the Enterprise Console

Execute the **PRTG Enterprise Console.exe** to start the Enterprise Console. As soon as it opens, the Enterprise Console tries connecting to your PRTG installation, according to the defined PRTG server connection settings. In a fresh install of PRTG, the settings for the Enterprise Console installed on the computer running the PRTG core server are already predefined, so you can use the Enterprise Console right away. If you get an error message when opening the Enterprise Console, please [check the connection settings](#)³⁴³¹. For example, adjusting the settings is necessary if you changed the IP address of the server.

 For detailed information, see section [PRTG Servers](#)³⁴⁶³ (**PRTG Server Connection**).

Tray Window

By default, the Enterprise Console runs in background and shows a message box whenever there are new alerts, new messages, or new tickets for your monitoring. This window is one of the first things you see after opening the Enterprise Console.



Enterprise Console - 31 Alarms and Warnings (common.strings.lastscan 16.10.2017 10:15:05)

PRTG NETWORK MONITOR New Alarms 2 New Log Entries 3 !! 20 W 11 ✓ 96 || 23 ? 3

Date Time	Parent	Object	Status	Message
16.10.2017 10:14:55	Probe Device	System Health	Warning	89 % (System CPU Load) is
16.10.2017 10:14:53	Cluster Probe Device	System Health	Warning	89 % (System CPU Load) is
16.10.2017 10:14:08	Probe Device	Windows Updates Status	Up	18 m 30 s
16.10.2017 10:13:55	Probe Device	System Health	Down	100 % (System CPU Load) is
16.10.2017 10:13:53	Cluster Probe Device	System Health	Down	100 % (System CPU Load) is
16.10.2017 10:13:39	Probe Device	SSL Certificate Sensor (Port	Warning	Warning by lookup value 'No'
16.10.2017 10:13:39	Aficio MP 301 (Ricoh Printer)	Hardware Status: RICOH	Warning	Warning by lookup value
16.10.2017 10:13:36	Exchange: nue-exmgmt-01	SSL Certificate Sensor (Port	Warning	Warning by lookup value 'No'
16.10.2017 10:13:31	Probe Device	RDP (Remote Desktop)	Up	44 msec
16.10.2017 10:13:27	Aficio MP 301 (Ricoh Printer)	Pages Printed Difference 1	Up	< 0,01 Pages/s
16.10.2017 10:13:27	Probe Device	Probe Health	Up	100 %
16.10.2017 10:13:25	Cluster Probe Device	Probe Health	Up	100 %

Alarms: 20 (2 new)
 New Log Entries: 3
 New tickets: 0

OK

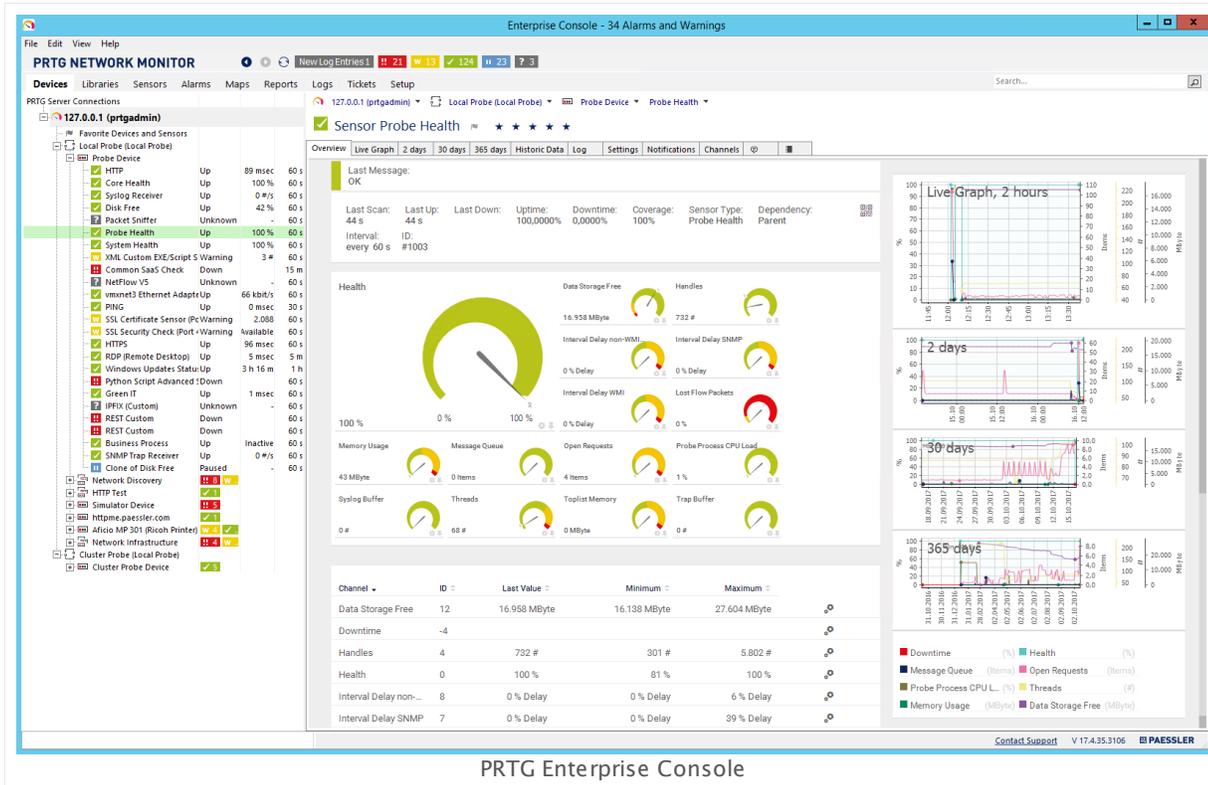
Example of the Tray Window

This window is always shown on top. Click the **OK** button to close it. You can change the tray behavior in the Enterprise Console settings.

 For detailed information, see section [Options](#)³⁴⁶⁸ (**System—Alerting**).

9.2 General Layout

The main layout of the Enterprise Console (EC in short form) program consists of different elements. See below for details.



PRTG Enterprise Console

From top to bottom, the main layout consists of:

- The [Windows menu](#)^[3435].
- The [page header bar](#)^[3435] with the PRTG logo, the viewpoint arrow symbols, the refresh icon, and the sensor states overview.
- The [menu tabs bar and page content](#)^[3435] underneath.
- The [server selection](#)^[3436] and [search bar](#)^[3436] in the upper right corner.
- The [news feed](#)^[3436] underneath the page content.
- The [status bar](#)^[3437] at the bottom of the window.

Often, the Enterprise Console displays data and settings directly. Some functionalities and extended setup additionally require a new window of the system's default browser and the [web interface](#)^[166] shows up. In this case, you are logged in to the web interface automatically via username and [hash value](#)^[3304]. In your browser, it might be necessary to confirm the certificate that is used by the PRTG web server.

For more information, see [SSL Certificate Warning](#)^[172] section.

If you configure your Enterprise Console for a connection with more than one PRTG core server, keep an eye on the [server selection](#)^[3436] bar to choose which server's data you want to access.

Windows Menu

The Windows menu gives access to general configuration and settings. For details, see section [Windows Menu Structure](#)^[3472].

Page Header Bar



The page header consists of the following parts:

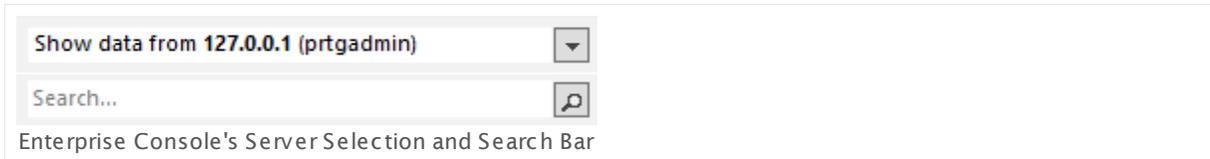
- **PRTG Logo**
Click the PRTG Network Monitor logo to open the [Ajax web interface](#)^[166] in the browser that you define in the Enterprise Console [Options](#)^[3466]. If you configured several PRTG core servers, the browser loads the web interface of the server that you have currently selected in the [Devices](#)^[3439] tab.
- **Previous Viewpoint / Next Viewpoint (Arrow Symbols)**
The Enterprise Console stores the different views that you navigate to in the application. Using these arrows (or using the shortcuts **Alt+Left** and **Alt+Right**), you can step back and forth in the history, just as you know from your web browser.
- **Refresh (Arrow Circle Symbol)**
Click the refresh symbol (**F5**) any time to refresh the current screen. This immediately queries data for the current screen from all active PRTG core servers just as the automatic refresh does. You can configure the update interval in the [Options](#)^[3466] settings.
- **Global Sensor Status Symbols**
This area shows the aggregated status of all sensors from all active PRTG core servers, divided into different sensor states. Depending on the particular sensor states, you see colored boxes with numbers, which symbolize the sensors. For example, you can see how many sensors are in **Up**, **Down**, **Warning**, **Pause**, **Unusual**, or **Unknown status**^[195]. Click a status icon to view a list of all sensors in the respective status.
Next to the global sensor status symbols you can also see the number of new alarms and new log entries, as well as the number of new tickets, if there are any. Click the respective icons to view [Alarms](#)^[219], [Logs](#)^[228], or [Tickets](#)^[230].
i When you view sensor lists, you can only show the sensors of one server at once. So, the global sensor overview shows the total number of sensors in a certain status on all active servers, but viewing a list of all sensors in a certain status from all servers is not possible for performance reasons.

Menu Tabs Bar and Page Content

You can navigate through your setup using the menu tabs bar. Please take a few minutes to familiarize yourself with all menu items. The page content underneath varies depending on the selected menu tab. It shows various information about your monitored objects.

 For a detailed description of all tabs, see section [Menu Tabs and Page Content](#) .

Server Selection



In the server selection bar you see all active PRTG core server connections that are configured for the current Windows user account (saved in the registry).

The server you select here determines globally which information the EC shows in all [Menu Tabs](#)  (except the **Devices** tab: the server selection does not apply for the devices tab). Depending on your selection, **Libraries**, **Sensors**, **Alarms**, **Maps**, **Reports**, **Logs**, **Tickets**, and **Setup** options are shown for the respective server only. Select **All PRTG Servers** to show consolidated information for all active PRTG core servers that appear in the list.

 For technical reasons, you cannot show consolidated information from all servers in the **Sensors**, **Setup**, and **Search Results** tab. To use these tabs, please select one single PRTG core server from the server selection bar.

Select **File | Manage PRTG Server Connections** from the [main menu](#)  to add or remove [PRTG Servers](#)  from the list, or to edit an existing one.

Search Bar

Select a single PRTG core server from the [server selection](#)  bar and enter a key word to search the respective server. In the **Search Results** tab, the Enterprise Console displays matching monitoring objects, help topics, and related objects. If you click a monitoring object (for example, a sensor) in the search results, the Enterprise Console opens this object on the [Devices](#)  tab with details in the device tree.

 If you have configured a connection in the [PRTG Servers](#)  options that uses a [Root ID](#)  other than 0, the EC will ignore this setting while searching. In this case, the EC shows **Search Results** for the entire server (starting at Root ID 0).

News Feed Bar

The news feed bar shows latest news by Paessler. Click the bar to open a window with an overview about recent articles. You can open a specific article in the web browser by clicking the particular header. If you do not want to show the news feed in your Enterprise Console, click the **X** symbol besides the bar. You can enable it again via **View | Show News Feed** in the [main menu](#)  (**Ctrl+N**).

Status Bar

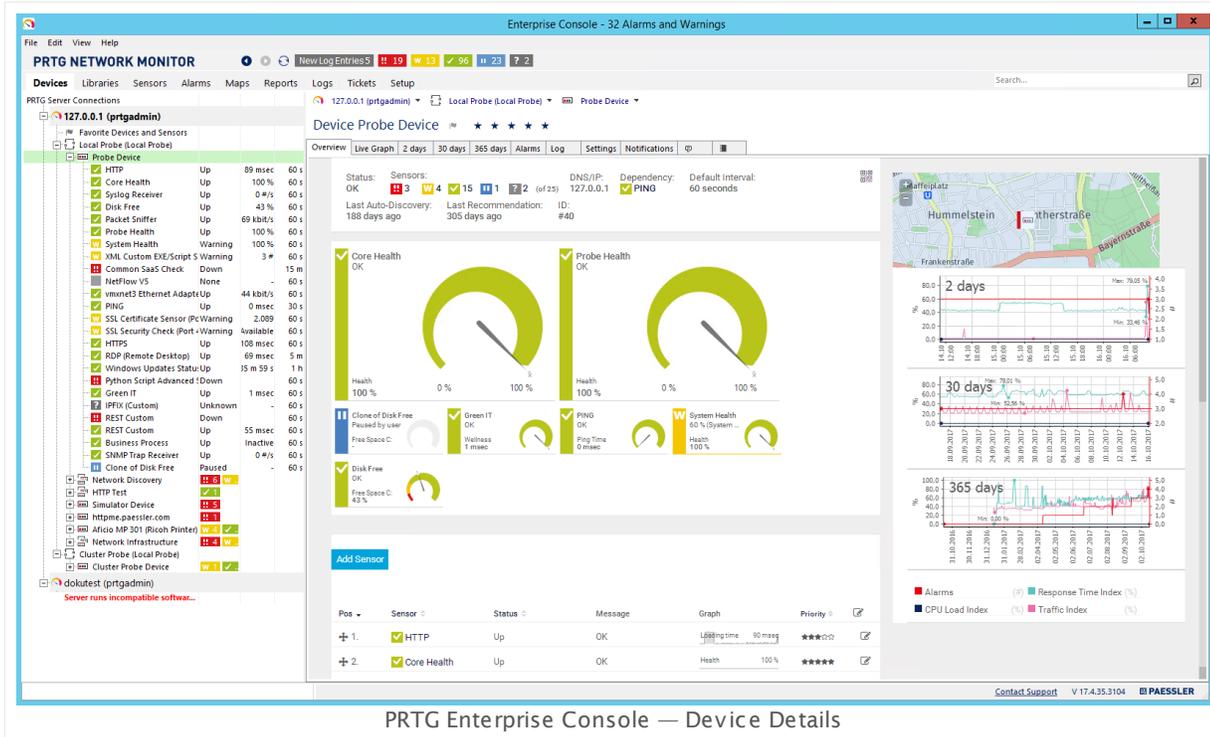


The status bar shows the version number of your PRTG Enterprise Console and the Paessler logo, which leads you to the Paessler website when you click it. Furthermore, the status bar contains a [Contact Support](#) link that opens a window to leave feedback or to ask for support.

You will also see a note if an update for one of connected servers is available. Click **Update Available** to open the [Auto-Update](#) page in the EC.

9.3 Menu Tabs and Page Content

Under the different menu tabs of the Enterprise Console, you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example.

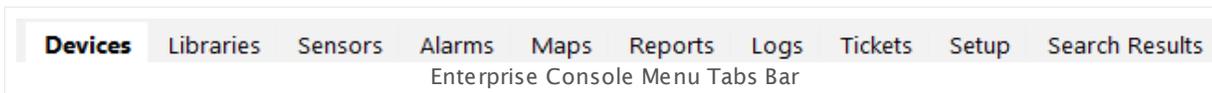


The following sections introduce the available options within the different tabs:

- [Devices](#) ³⁴³⁹
- [Libraries](#) ³⁴⁴⁶
- [Sensors](#) ³⁴⁴⁸
- [Alarms](#) ³⁴⁵⁰
- [Maps](#) ³⁴⁵²
- [Reports](#) ³⁴⁵⁴
- [Logs](#) ³⁴⁵⁶
- [Tickets](#) ³⁴⁵⁸
- [Set up](#) ³⁴⁶⁰
- [Search Results](#) ³⁴⁶²

9.3.1 Devices

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Devices Menu Tab

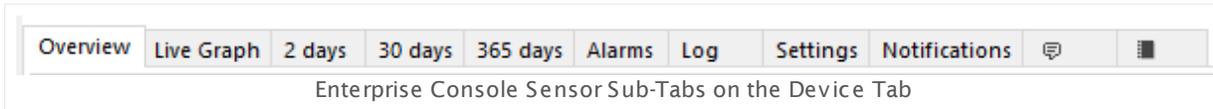
The **Devices** tab is your starting point for everyday use. The page is split into two parts. On the left hand side, it shows the tree-like device view that lists all configured PRTG core servers with their probes, groups, devices, and the sensors on the devices, in a hierarchical order. Next to each object you see an overview of the number of sensors, grouped by their current status.

The first child node of the tree is called **Favorite Devices and Sensors**. It contains all devices and sensors that you marked as [favorites](#)  242. To add an object to the favorites list, right-click the desired device or sensor and select the **Add to Favorites** entry from the [context menu](#)  247.

 For more information about the hierarchical order of the different objects in the device tree, see section [Object Hierarchy](#)  133.

On the right side you see details about the object selected on the left. The information is spread over several tabs.

Over the object's name you see always a path that you can use to navigate through the device tree. It can also help you to orient yourself if you get lost. If you click a **breadcrumb** item, a dropdown menu opens that shows all available objects on the same level. For example, you can use this to directly access all other sensors or a device, other devices within a group, another group on the same probe, other probes in your root group, or another PRTG server.



Edit Objects in the Device Tree

Use the **Edit** menu (or the object's [context menu](#)³⁴⁸⁰) to access different important functions of the items you have currently selected in the device tree on the left hand side.

- Add devices or sensors to the favorites list (or remove them from the list)
- Sort all sub nodes of an object alphabetically
- Move objects up and down in the tree
- Scan now
- Pause monitoring
- Access tools
- and many more

 For details about the available options, see section [Windows Menu Structure](#)³⁴⁷².

Select Multiple Items in Device Tree

In the device tree shown on the left, you can select one or more objects, even from different PRTG core servers. Hold down the **Ctrl** key to select more objects simultaneously with your mouse. Usually, you select more than one item to view combined graphs, or to apply a command from the [Windows Menu](#)³⁴⁷² (for example, **Scan Now** or **Pause**) to several objects.

When you select multiple items, the sub-tabs on the right side show data for **all** selected items at a glance. For example, when if you select two sensors, you see their tables next to each other. Graphs will actually appear combined! This is a great way to instantly show one chart containing the graphs of all selected objects. Each sensor channel is represented as one line. This aggregated view works for all kind of objects.

-  The tab **Live Graph** shows data for sensors only.
-  Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.



Aggregated Graph View in Enterprise Console

i You may need to enlarge the Enterprise Console's window to see all tables and graphs.

Devices—Overview

The **Overview** tab shows general information about the selected object. Depending on the selected object selected, you can see different information.

- For **servers**, **probes**, and **groups** the table shows information in the **Name** and **Status** section, such as priority, parent objects and number of sensors on this object. Additionally, the window shows a geographical map, if enabled in your PRTG configuration as well as in the Enterprise Console's **View** ³⁴⁷⁷ menu, and **index graphs** ²⁰⁰¹.
 For detailed information about geographical maps, see section **Geo Maps** ³²¹¹.
- For **devices**, the **Overview** tab shows device details and summary graphs for different time spans, gauges, as well as a list of all sensors on this device, **recommended sensors** ²¹³, and a geo map.
- For **sensors**, the **Overview** tab shows sensor details, current status, and the last value of all sensor channels, as well as sensor graphs for different time spans. You can also edit channel settings in this tab by clicking on a channel's gear icon.
 For details, see section **Sensor Channels Settings** ³¹⁶⁰.

Devices—Live Graph, 2 days, 30 days, 365 days

These tabs are only available if you enable the **Large Single Graph** (Ctrl+L) view in the [Windows Menu](#) (View).

For **Small Multiple Graphs** view, see section [Devices—Graph](#) below.

Select one of the tabs to display an object's monitoring results as **Live Graph** (content available for sensors only), or for different time spans in more or less detail (**2 days**, **30 days**, **365 days**). On every tab, you will see graphs as well as data tables.

While you view a sensor graph, you can hide single sensor channels individually. Remove the check mark symbol in front of a channel name underneath the graph, and the line of the according channel disappears. You can also **Show all** or **Hide all** channels by clicking these buttons in the graph. The graph view is reset immediately.

- The days mentioned here are the default setting. You can change the detail of the different graphs any time under [System Administration—User Interface](#).
- Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.

Devices—Graph

This tab is only available if you enable the **Small Multiple Graphs** (Ctrl+S) view in the [Windows Menu](#) (View). For **Large Single Graphs** view please see [above](#). This tab shows an overview with single graphs and data tables for live data, 2 days, 30 days, and 365 days. It might be necessary to enlarge the window to display all graphs.

- The days mentioned here are the default setting. You can change the detail of the different graphs any time under [System Administration—User Interface](#).
- Below each graph you see a key. Hover over an entry in the key to display the corresponding line in the graph above in **bold**.

Devices—Historic Data

The **Historic Data** tab is available for sensors only (not for probes, groups, or devices). When you open the historic data tab of a sensor, there is no sensor selection available. If you want to select a different sensor for the report, select **Sensors | View Historic Data** from the main menu in the PRTG web interface.

Historic Data Tab of Ping Sensor

Select the **File Format** for the results:

- **HTML web page:** Opens a new browser window with the historic data report
- **XML file:** Opens a new browser window with the historic data report as XML file.
- **CSV file:** Opens a new browser window with the historic data report as CSV file.

i When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)^[3470] will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, find more information in section [SSL Certificate Warning](#)^[172].

📖 View and functionality are the same as in the web interface. For details about the available **Historic Data** report options, see section [Historic Data Reports](#)^[204] of the [Ajax Web Interface](#)^[166] documentation.

Devices—Log

Click the **Log** tab to show a table list with all log information **on this object**. This is a subset of the entries available via the [Logs](#)^[3456] menu tab.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

Devices—Settings

The **Settings** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface. For every type of object and for every sensor, different options are available. For detailed information, see the following sections (depending on the selected object) in the [Ajax Web Interface](#)^[166] documentation:

- [Probe Settings](#)^[351]
- [Group Settings](#)^[375]
- [Device Settings](#)^[402]
- [Sensor Settings](#)^[428]

Devices—Settings—Multi-Edit

If you select several objects on the left side, the **Settings** tab switches into [multi-edit mode](#)^[3197]. Using multi-edit, you can set a check mark for one or more settings. All changes apply to all selected objects. The multi-edit dialog displays settings that are common among the selected objects only.

If you select only sensors on the left side in the device tree, the **Settings** tab additionally displays a **Channel Settings** tab. Using this tab you can multi-edit the [settings of any channels](#)^[3160] that are common among the selected sensors, as long as the channels have the same name. Set a check mark for one or more channel settings. All changes apply to all selected sensors.

 You cannot use multi-edit for objects on different PRTG core servers.

Devices—Notifications

The **Notifications** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface. You can set different notification triggers.

 For detailed information, see section [Sensor Notification Triggers Settings](#)^[3170] in the [Ajax Web Interface](#)^[166] documentation.

 You cannot change notification settings for multiple objects at a time. We recommend that you use the [Inheritance of Settings](#)^[137] for easy configuration.

Devices—Comments

The **Comments** tab loads and displays the currently selected object's settings from the web interface. View and functionality are the same as in the web interface.

On the **Comments** tab you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

Save your settings. If you change tabs or use the main menu, all changes to the settings will be lost!

Devices—History

The **History** tab shows all changes to the settings of an object with a timestamp, the PRTG user that conducted the change, and a message.

Drag & Drop Sorting in Device Tree

In the device tree, you can also move probes, groups, and devices simply via drag and drop. Activate it in the [Windows menu](#)^[3472] under **Edit | Drag & Drop Sorting** and then drag your objects as you like: You can move devices and groups, or add groups or devices to other groups. You can also move objects via the [context menu](#)^[3480].

You cannot move objects in the following cases:

- You cannot move any objects from one PRTG core server to another.
- You cannot move sensors from one device to another. To clone sensors to other devices using drag & drop, please use the [Ajax Web Interface](#)^[166].
 For detailed information, see section [Manage Device Tree](#)^[329].
- You cannot move devices from one group to another.
- You cannot move groups from one probe to another.
- You cannot move probes from one core server to another.

9.3.2 Libraries

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#) 
- [Libraries](#) 
- [Sensors](#) 
- [Alarms](#) 
- [Maps](#) 
- [Reports](#) 
- [Logs](#) 
- [Tickets](#) 
- [Setup](#) 
- [Search Results](#) 

Using Libraries is a great way to keep an eye on your network status because you can individually select which sensors you would like to see there.

 For a general introduction to PRTG Libraries, see section [Libraries](#) .

Libraries Menu Tab

The page is split into two parts. On the left hand side you see all available libraries from one or several servers, on the right hand side the actual libraries.

- Click a library's name to display it. In the tabs above the library, select from [Overview](#) , [Management](#) , [Settings](#) , [Notifications](#) , [Comments](#) , and [History](#) . Each of these tabs loads the respective functionality of the [Ajax Web Interface](#) . Click the **Save** button to apply changes to your settings.
- Underneath the tabs bar, there are different options available to change the current library view: You can set sensor filters (set or remove check marks to include or exclude sensors in a certain status) and change the device tree view.
 -  For details about the tree view, see section [General Layout—Tree View Layout](#) .
- Click a library node to edit the [node settings](#)  in a new window.

- Double-click a library's name on the left to open the library in the configured external web browser. You can edit it or add new libraries to this PRTG server.
- Right-click a library's name to open its [context menu](#)^[3480]. The following options are available: **Add**, **Edit**, **Delete**, **Clone**, **Send link by email**, and **Open in Web Browser** in the libraries overview on the left **Edit**, **Delete...**, **Add Library Node...**, **Add Group...**, and **Send Link by Email** on the **Overview** tab of a specific library on the right.
- Use the button **Add Library** to create a new library and the button for [object history](#)^[273] to view all changes to libraries.

 For more details about PRTG Libraries, see section [Libraries](#)^[3235].

Libraries Menu Tab—Add Library

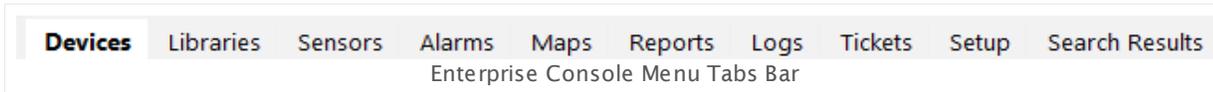
Click the **Add Library** button to add a new library to a PRTG server.

Depending on the current setting shown in the [server selection](#)^[3436] bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

 For details about adding a library, see section [Libraries Step By Step](#)^[3238].

9.3.3 Sensors

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Viewing lists of sensors is a great way to keep an eye on your network status because you can select which kind of sensors you want to see. You can filter by various parameters like object or sensor type, for example, and current sensor status.

Sensors Menu Tab

 For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

Click the **Sensors** entry in the menu tabs bar to show a table list of all sensors. You can enable a filter to only show certain sensors. To do so, choose from three different dropdown menus to build a filter. With each filter you can further decrease the number of shown sensors.

- **By Type**
The second dropdown menu shows [all sensor types](#)  429 available in your monitoring setup. Select an entry to only show sensors of this type. The default value is **All Sensors**.

- **By Status**

The third dropdown menu shows all possible [sensor states](#)¹⁹⁵. Select an entry to only show sensors that currently show this status. Choose between **All States**, **Down**, **Down (Acknowledged)**, **Down (Partial)**, **Warning**, **Up**, **Paused**, **Unusual**, and **Unknown**. The default value is **All States**.

 If you click a sensor symbol in the [page header bar](#)^{343b}, you can directly view a sensor list filtered by the selected sensor status for the selected server.

If you have filtered out all sensors and the list below shows no entries, remove some filters by reverting them to the default values.

 In the column **Last Value**, the table only shows the last value of the sensor's **primary channel**.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

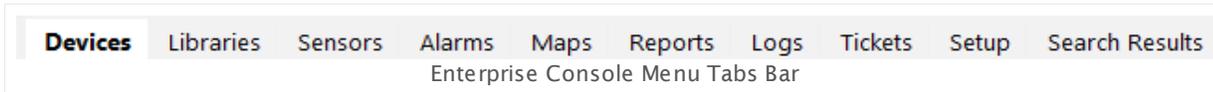
From this list view, you can select multiple items to apply the same action to them, for example, **Edit** | **Scan Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while pointing to the lines you want to select
- Hold the **Ctrl** key while clicking to toggle the selection status of a single line
- Click a line and hold the **Shift** key while clicking another line to select all lines in between.

9.3.4 Alarms

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Alarms Menu Tab

In the **Alarms** tab you can show the alarms of **all** active PRTG core servers. To do so, select **All PRTG Servers** from the server selection in the upper right corner.

The alarms list shows all sensors that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** status. Sensors in other states (for example, **Up**, **Paused**, or **Unknown**) do not appear here. This is useful for keeping track of all irregularities in your network.

Using the options **Error**, **Warning**, and **Unusual**, you can hide and show sensors in the respective status by removing and adding a check mark. When choosing **Error**, this includes sensors in the states **Down**, **Down (Partial)**, and **Down (Acknowledged)**.

Click **Show as Gauges** to show the sensors on the **Alarms** tab represented with [gauges](#)  198.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

From this list view, you can select multiple items to apply the same action to them, for example, **Edit** | **Scan Now**.

You can select multiple items by the following means (you can also combine them):

- Click and hold your left mouse key while pointing to the lines you want to select
- Hold the **Ctrl** key while clicking to toggle the selection status of a single line
- Click a line and hold the **Shift** key while clicking another line to select all lines in between.

Acknowledge Alarm

An acknowledged alarm shows up in the alarms list as "acknowledged" (see [Sensor States](#)^[195]) and will not [trigger](#)^[3170] any more [notifications](#)^[3216].

- ❗ If the alarm condition clears, the sensor usually returns to an **Up** status immediately with the next sensor scan.

To acknowledge an alarm, right-click a sensor entry and choose **Acknowledge Alarm...** from the context menu, enter a message and click the **OK** button. The message will appear in the last message value of the sensor. You can choose between: **Acknowledge Indefinitely...**, **acknowledge For 5 Minutes...**, **For 15 Minutes...**, **For 1 Hour...**, **For 3 Hours...**, **For 1 Day...**, or **Until...**

If you choose **Until...** a dialog box appears:

ACKNOWLEDGE ALARM UNTIL

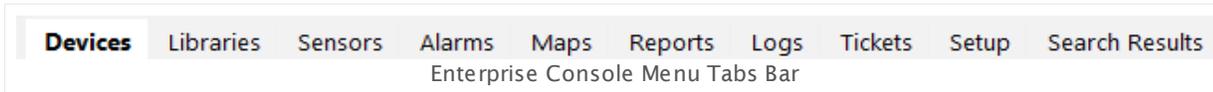
Selected Objects	Shows the sensor(s) that you want to acknowledge the alarm for. You can acknowledge alarms for more than one sensor using multi-edit ^[3197] .
Message	Enter a text, for example, the reason why you acknowledge the alarm. Please enter a string or leave the field empty.
Until	Enter the date when the acknowledge status will end. Use the date time picker to enter the date and time.

❗ If the alarm condition still persists after the specified date, the sensor will show a **Down** status again.

Only [users](#)^[3376] with write access rights may acknowledge alarms. You can give read-only users the right to acknowledge alarms, too. See section [User Accounts Settings](#)^[3377], section **Account Control**.

9.3.5 Maps

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Maps Menu Tab

The page is split into two parts. On the left hand side you see all available maps from one or several servers, on the right hand side the details of the selected map.

- Click a map's name to display it. In the tabs above the map, select from **View Map**, [Map Designer](#)  3287, [Settings](#)  3297, [Get HTML](#)  3300, [Comments](#)  3301, and [History](#)  3301. Each of these tabs loads the respective functionality of the [Ajax Web Interface](#)  166. Remember to click the **Save** button to apply your settings.
- Double-click a map's name to open the map in the configured external web browser. You can edit it using the [Map Designer](#)  3287, or add new maps to this PRTG server.
- Right-click a map's name to open a [context menu](#)  3480. The following options are available: **Add**, **Edit**, **Delete**, **Clone**, **Send Link by Email**, and **Open in Web Browser**.
- Use the **Add Map** button to create a new map and the button for [object history](#)  273 to view all changes to maps.

 For more details, see section [Maps](#)  3276.

Maps Menu Tab—Add Map

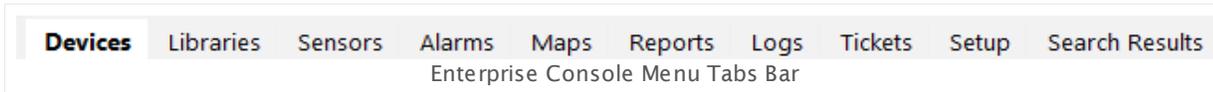
Click the **Add Map** button to add a new map to a PRTG server.

Depending on the current setting shown in the [server selection](#)  bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

 For details about adding a map, see section [Maps Step By Step](#) .

9.3.6 Reports

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Reports Menu Tab

On the **Reports** tab you see all available reports from one or several servers in one list.

If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click once or twice on the header of the column you want to sort by.

Choose one report and double click its name to open its details. The page will split into two parts. On the left hand side you see all available reports from one or several servers, on the right hand side the options for the currently selected report.

- Click a report's name in the list on the left to display its options. In the tabs above the report, select from [Run Now](#)  3261, [Stored Reports](#)  3264, [Settings](#)  3265, [Select Sensors Manually](#)  3275, [Sensors Selected by Tag](#)  3276, and [Comments](#)  3277. Each of these tabs loads the respective functionality of the [Ajax web interface](#)  166. Remember to click the **Save** button to apply your settings.
- Right-click a report's name to open its [context menu](#)  3480. The following options are available: **Add**, **Run Now**, **Edit**, **Delete**, **Clone**, **Send Link by Email**, and **Open in Web Browser**.
- Use the **Add Report** button to create a new report and the button for [object history](#)  2731 to view all changes to reports.

 For details, see section [Reports](#)  3252.

Reports Menu Tab—Add Report

Click the **Add Report** button to add a new report to a PRTG server.

Depending on the current setting shown in the [server selection](#)  bar in the upper right corner, an (embedded) window will open (if one specific server is selected), or you will see a selection window that asks you to choose the core server you want to add the new item to. Choose an installation to start.

 For details about adding a report, see section [Reports Step By Step](#) .

9.3.7 Logs

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Logs show all past activities and events of your PRTG monitoring setup. This is useful for researching past user activities, system events, and, for example, to check whether messages were sent. In a typical setup, a huge amount of log data is produced. Because the activity of every single object is recorded, you can use this information to check if your setup works exactly as desired.

There are two options to call the logs list: Either you click the **Log** tab while you view an object's details on the [Devices](#)  3443 menu tab, or you choose the **Logs** entry from the menu tabs bar.

Logs Menu Tab

Click the **Logs** entry in the menu tabs bar to show a list of **all** log entries of a PRTG core server.

You can either view the entries of one or all servers. If you have configured more than one PRTG core server and you want to view entries from all servers in your [PRTG Servers](#)  3463 setup, simply select **All PRTG Servers** from the server selection in the upper right corner.

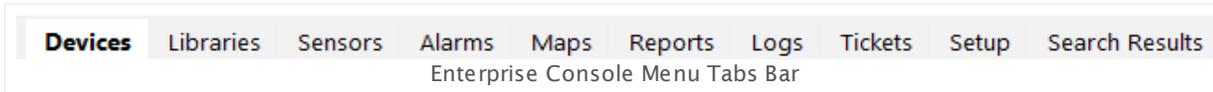
You can enable a filter to only show log entries of a certain event from the categories **Status Changes**, **System Events**, and **Object History**. Choose a category from the **Show** menu. The second dropdown menu shows all possible event types for the selected category. Select an entry to only show events of the respective event type. Choose a [sensor status](#)^[195] for status changes, **Probe Related**, **Auto Discovery**, **Notifications**, or **Status Messages** for system events, or a [system object for object history](#)^[229].

You can also define the time span for which you want to show logs. Use the date time picker to enter the date and time.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

9.3.8 Tickets

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Tickets Menu Tab

 For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

On the **Tickets** tab you can view all tickets on the currently selected PRTG core server.

 You can only display tickets from one server at the same time, not from all PRTG servers.

In the header bar of the tickets list, you can choose several filters to find and display certain tickets: by status, type, concerned user or user group, related monitoring objects, and last edit. Click the **X** symbol to undo the date selection.

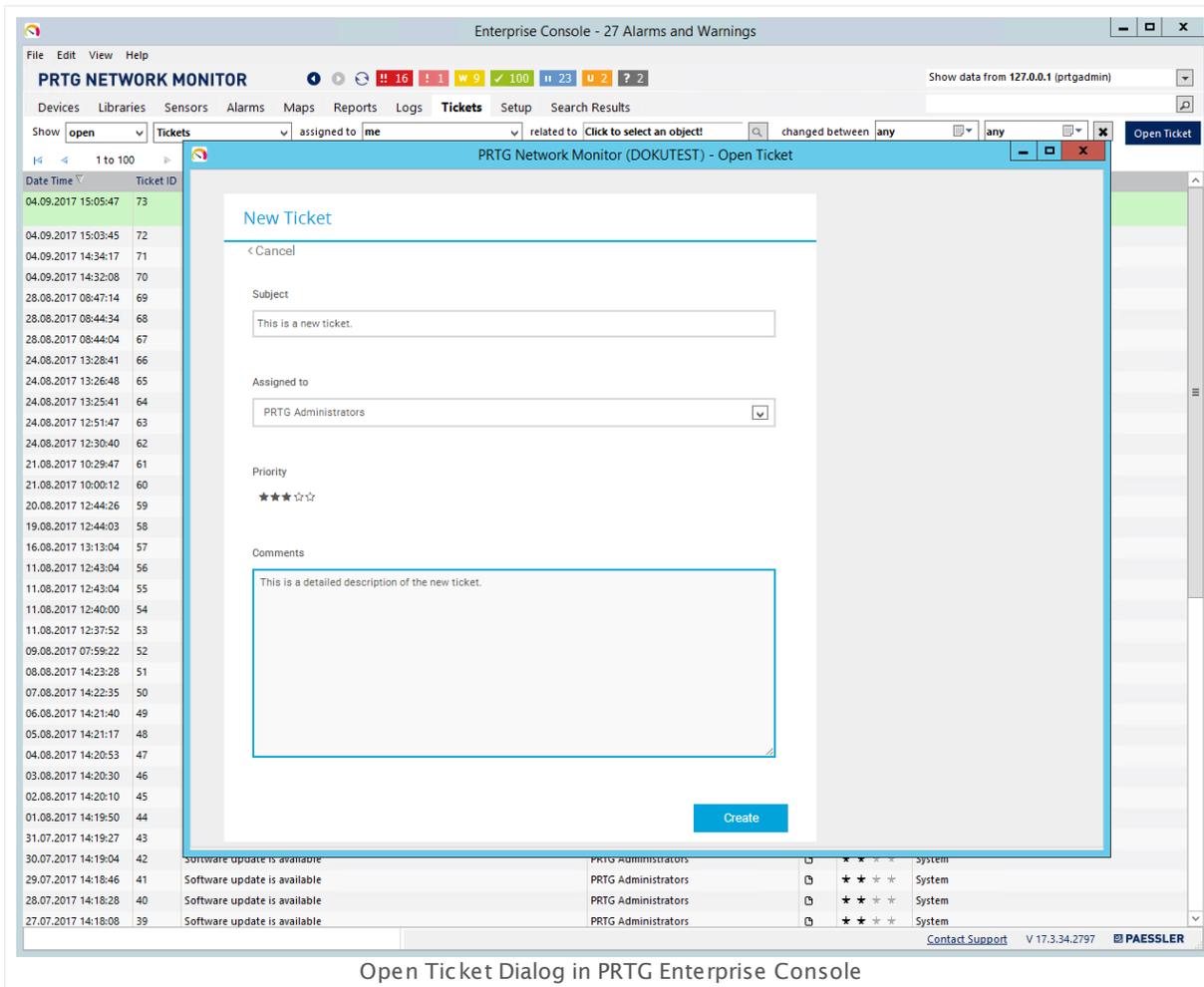
Double-click an entry in the tickets list to open a ticket in a new window and to conduct ticket related actions (edit, assign, resolve, close, or reopen). You can also multi-edit tickets via the context menu: mark several tickets by holding **Ctrl** or **Shift** and clicking on the corresponding tickets. **Right-click** a ticket to open the context menu.

The following actions are available: **Open Ticket**, **Edit Ticket**, **Assign Ticket**, **Resolve Ticket**, **Reopen Ticket**, **Close Ticket**, **Priority/Favorite**, **Open in Web Browser**.

The list can show up to one hundred entries at a time. Use the arrow symbols above the list to show other items. You can jump to the beginning of the list, or browse through it hundred by hundred. If the list has more than one entry, you can also sort the items by the contents of a certain column. To sort, simply click the header of the column you want to sort by once or twice.

Tickets Menu Tab—Open Ticket

To open a new ticket, click **Open Ticket** in the upper right corner or in the context menu. Select a related object, click **Continue**, and provide **Subject**, **Assigned to**, **Priority**, and **Comments**. Once finished, click **Create** to create the ticket.



Open Ticket Dialog in PRTG Enterprise Console

For details about working with the PRTG ticket system, see section [Ticket s](#) ²³⁰ for the PRTG web interface.

9.3.9 Setup

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Setup Menu Tab

 For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

On the **Setup** tab you can access all options available in the [Setup](#)  3302 menu of the Ajax web interface. You can collapse and expand the sections by clicking the **-** or **+** symbol.

For more information, refer to the respective section in the documentation for the PRTG web interface.

Account Settings:

- [My Account](#)  3304
- [Notifications](#)  3311
- [Notification Contacts](#)  3334
- [Schedules](#)  3338

System Administration:

- [User Interface](#)  3343

- [Monitoring](#) 
- [Notification Delivery](#) 
- [Core & Probes](#) 
- [Administrative Tools](#) 
- [Cluster](#)  (available in a [cluster](#)  setup only)

User Accounts:

- You see a list of configured user accounts. Select one to change settings. For details, see [User Accounts](#)  section.

User Groups:

- You see a list of configured user groups. Select one to change settings. For details, see [User Groups](#)  section.

PRTG Status:

- [System Status](#) 
- [Cluster Status](#)  (available in a [cluster](#)  setup only)
- [Licensing Status and Settings](#) 
- [Auto Update](#) 

Optional Downloads and Tools:

- [Client App for Windows \(Enterprise Console\)](#) 
- [Client Apps for Mobile Devices](#) 
- [Remote Probe Installer](#) 

Support:

- [Contact Support](#) 

9.3.10 Search Results

The Enterprise Console has a tab-like interface. Using the tabs you can navigate through various pages with information about your monitored objects, such as your network status and monitoring results, for example, as well as access maps, reports, tickets and settings.



There is documentation available for the following tabs:

- [Devices](#)  3439
- [Libraries](#)  3446
- [Sensors](#)  3448
- [Alarms](#)  3450
- [Maps](#)  3452
- [Reports](#)  3454
- [Logs](#)  3456
- [Tickets](#)  3458
- [Setup](#)  3460
- [Search Results](#)  3462

Search Results Menu Tab

 For technical reasons, this function is available for one server at a time only. If you have configured more than one PRTG core server, choose one server from the server list in the upper right corner.

The **Search Results** tab is only visible if you do a search using the search box in the upper right corner. For your search, the Enterprise Console shows all matching objects on one PRTG core server. Click a monitoring object in the results to show it in the Enterprise Console's [Devices](#)  3439 tab.

Other objects, for example, manual sections, load in an external browser window.

 When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)  3470 will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, find more information in section [SSL Certificate Warning](#)  172.

9.4 PRTG Servers

The Enterprise Console connects to the web server API running on every PRTG core server installation. It supports saving the configuration for a connection to one or more PRTG core servers. In a full PRTG installation, there is already a connection predefined.

i For a successful connection, the program versions of Enterprise Console and PRTG core server have to match. When connecting to several servers, make sure they all run on the same software version. At least the third number of the whole version number has to be equal. For example, EC version 17.2.31.1917 can connect to server version 17.2.31.2018.

PRTG Servers List

From the main menu, select **File | Manage PRTG Server Connections** to view a list of all servers configured for the currently logged in Windows user account. You can also access this list by clicking the **PRTG Server Connections** entry above the device tree.

All PRTG Server Connections

Add PRTG Server Connection
 Delete PRTG Server Connection
 Move Up
 Move Down

Active	PRTG Server	Status	Background Activity	Core Version
<input checked="" type="checkbox"/>	127.0.0.1 (prtgadmin)			17.3.34.2797
<input checked="" type="checkbox"/>	demo (prtgadmin)			17.3.34.2797+

PRTG Servers List in the Enterprise Console

The list shows the server or display name, as well as login information used. In the **Status** column you see an overall sensor status for this server connection. You can also see if there is any **Background Activity** on the respective server (for example, a running [Auto-Discovery](#) ²⁸²), which can potentially affect performance and response times.

In the list, set a check mark for every PRTG server you want to poll with every update interval. If a server is not reachable, the Enterprise Console deactivates it automatically after several unsuccessful connection attempts. When opening the Enterprise Console, it automatically re-establishes the connection to all active servers.

Add or Edit a PRTG Server Connection

- Click **Add PRTG Server Connection** in the header bar above the server list to add a new server connection configuration.
- Click **Delete PRTG Server Connection** to remove an entry from the list.
- Click **Move Up** or **Move Down** to change the order of the servers on the [Devices](#) ³⁴³⁹ tab.

There is also a [context menu](#) ³⁴⁸⁰ available for each server connection with the following options.

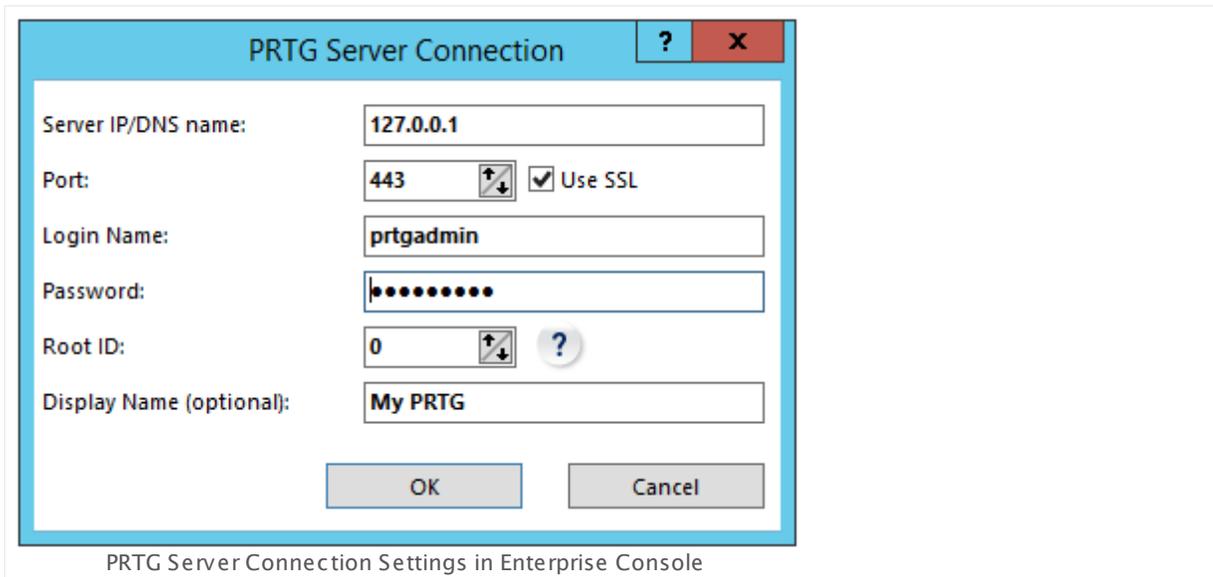
- Click **Deactivate PRTG Server Connection** to remove the server from the [Devices](#) ³⁴³⁹ tab but keep the server connection settings.
- **Add** a server.
- Open and edit the **Settings** of the server.

- **Delete** the server.
- **Move Up** and **Move Down** to change its position on the [Devices](#) tab.
- Open the server in the Ajax web interface (**Open in Web Browser**).

To change the settings of an existing server in the list, open its context menu with **right-click** and click **Settings** or click the respective wrench symbol in the table. You can alternatively use the context menu of a server on the [Devices](#) tab. There you can choose between **Edit PRTG Server Connection** to open the edit dialog, **Deactivate PRTG Server Connection** to not show this server's monitoring data anymore (you can later reactivate it in the [servers list](#)), or view [Dependencies](#).

When adding or editing, a dialog box appears to enter connection information.

- ❗ Connection settings are stored for each Windows user individually in the registry under the following node: `HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI`



Server IP/DNS name

- Enter the IP address or DNS name of the PRTG server the Enterprise Console connects to.
- This is the same address or name as defined in the web server settings for the core server. For detailed information, see [PRTG Administration Tool](#) (**Web Server**) section. Make sure the values match.
- Make sure the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings block the connection.

Port

- Enter the port on which the PRTG server runs.

- This is the same port as defined in the web server settings for the core server. For detailed information, see [PRTG Administration Tool](#) ³⁶⁶² (Web Server) section. Make sure the values match.
- Make sure the server is reachable (especially when using Network Address Translation (NAT)) and no firewall settings block the connection.

Login Name

- Enter the login name that you use to login to the web server.
- This can be the administrator login or the login of another PRTG user.
- In a new installation, the login name is **prtadmin** by default.
- For detailed information about user accounts, see [System Administration—User Accounts](#) ³³⁷⁶ section.

Password

- Enter the password for the login name entered above.
- In a new installation, the password is **prtadmin** by default.

Root ID

- Enter the ID of the object that is [the root of the device tree](#) ¹³³.
- Default value is **0**, which is the **Root** group of your configuration.
- If you enter an other object's ID here, the device tree will start at this object, only showing all other objects below in the hierarchy.
- This is useful to only view a part of the device tree, which might load much faster.
- You can create several connections that only differ in the **Root ID** value to quickly switch between different views within your configuration, choosing different PRTG core server connections in the Enterprise Console's [Devices](#) ³⁴³⁹ tab.

Display Name (optional)

- Optionally enter a name that the EC displays in the **PRTG Server Connections** list.
- If you leave this field blank, the Enterprise Console displays the **Server IP/DNS name** setting there.

Click the **OK** button to save your settings or **Cancel** to discard them.

9.5 Options

From the [Windows menu](#)  of the Enterprise Console, select **File | Options...** to open the options dialog.

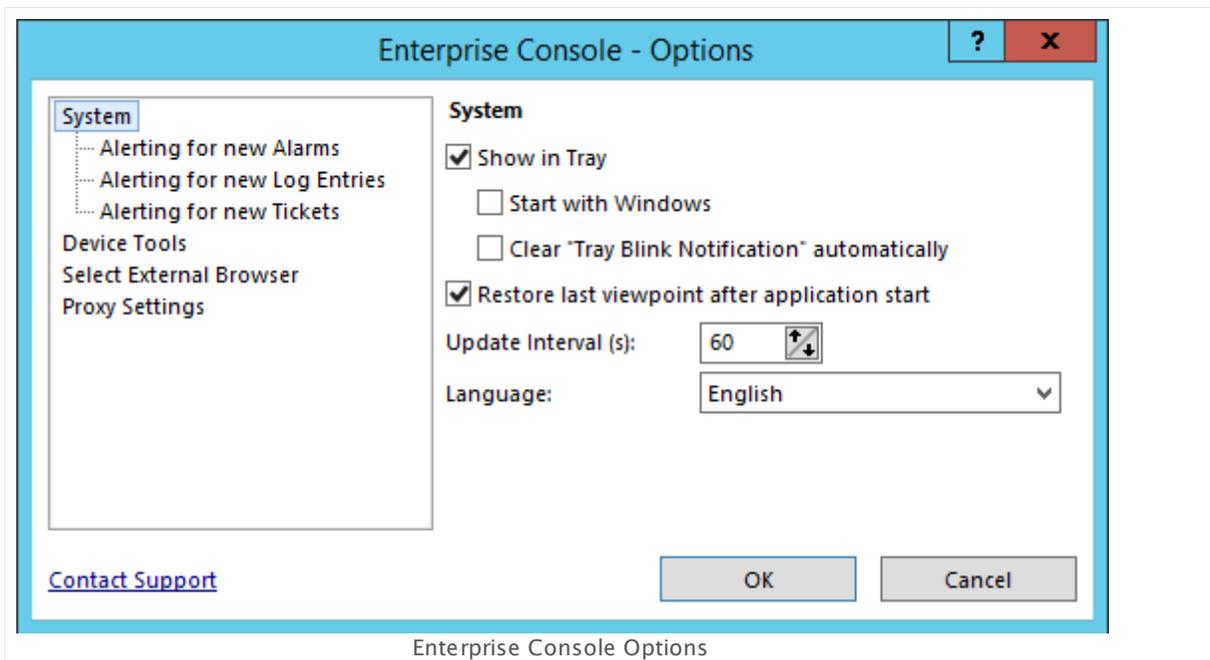
You can choose from these options on the left hand side:

- [System](#) 
- [System—Alerting](#) 
- [Device Tools](#) 
- [Select External Browser](#) 
- [Proxy Settings](#) 
- [Contact Support](#) 

System

From the [Windows menu](#)  of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

Change general system settings for the Enterprise Console.



ENTERPRISE CONSOLE – OPTIONS: SYSTEM

Show in Tray	<p>By default this setting is enabled. With this setting enabled, a PRTG icon appears in the Windows tray^[3433]. When you point your mouse to it, it will show information with the most important status information about your monitoring. With a right-click you can access a menu with access to the most important functions.</p> <p> To use any alerting functionalities (see System—Alerting^[3488] section), you must enable this option. If the tray icon is not shown, no alerting from the Enterprise Console is available.</p>
Start with Windows	<p>This setting is only available to change only if you enable the tray option above. By default this setting is enabled. With this setting enabled, the Enterprise Console will start up automatically when Windows starts.</p>
Clear "Tray Blink Notification" automatically	<p>This setting is only available to change only if you enable the tray option above. Whenever there are new entries in the Alarms^[3450] list, the tray icon will start blinking. If you enable this option, the tray icon will stop blinking automatically as soon as there are no more alarms.</p> <p> With this option disabled, the icon will keep blinking, even if all alarms are cleared meanwhile.</p>
Restore last viewpoint after application start	<p>If this option is enabled, the Enterprise Console saves information about the currently shown view (for example, sensor details, a certain graph, or a map^[3278]). It is written to the registry^[3471] when you close or exit the program. When you open the Enterprise Console again, it will try to restore the same view.</p> <p>Only if the object is not available any more (due to changes on the server, or due to unavailability of a server), the default view loads.</p>
Update Interval (Sec.)	<p>Define the number of seconds that the Enterprise Console waits before the screen refreshes. Please enter an integer value. Default value is 60 seconds. You can use the up and down arrows to go one second up or down.</p>
Language	<p>Choose the language for the Enterprise Console from the dropdown menu. Default is English. Depending on your installation, you can choose other languages here.</p> <p> This setting only influences the language of the Enterprise Console.</p>

System—Alerting

From the [Windows menu](#)³⁴⁷² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

You can define what the Enterprise Console will do in case of new **Alarms, Log Entries, or Tickets**. The settings are the same for all of these three cases, but you can individually define them for each case. On the left side, select either **Alerting for new Alarms, Alerting for new Log Entries, or Alerting for new Tickets** and define the settings as follows.

 All alerting options only take effect if you enable the **Show in Tray** option in the [system](#)³⁴⁶⁶ settings above. If the tray icon is disabled, there will be no alerting from the Enterprise Console.

ENTERPRISE CONSOLE - OPTIONS: ALERTING FOR NEW ALARMS

Blink Tray Icon	The tray icon will blink if there are new items to be alerted for. You can additionally set the Clear Tray Blink Notification automatically option in the system ³⁴⁶⁶ settings above.
Balloon Info in Tray	Show a balloon info next to the PRTG tray icon if there are new items to be alerted for.
Popup Message	Show a popup message window if there are new items to be alerted for.  The popup window will be always on top until it is closed.
Play Sound	Play an audible notification if there are new items to be alerted for. There is a default sound defined. To change it, click the folder icon and select any standard WAV file from your hard disk drive. PRTG already comes with a small set of sounds you can choose from.  The sound file is only played on the computer running the Enterprise Console.
Open Enterprise Console	Open the Enterprise Console if there are new items to be alerted for.

Device Tools

From the [Windows menu](#)³⁴⁷² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

In the **Device Tools** settings you can define commands that will be available in the [Windows Menu](#)³⁴⁷² and [context menu](#)³⁴⁸⁰ of groups, devices, and sensors. A command to initiate a remote desktop connection is already predefined.

 You may need to run the Enterprise Console as administrator to make the tool function work with your Windows version.

Click the **Add** button to add a new command, or choose an existing one from the list and click the **Edit** button to change the settings. Use the **Delete** button to remove an entry from the list.

ENTERPRISE CONSOLE – OPTIONS: EDIT TOOL

Name	Enter a custom name for your command. The command will show up with this name in context menus. Please enter a string.
Command	Enter the command you want to execute on the local machine. This can be, for example the name of a program or script, with or without path, according to your system's configuration.
Parameters	Enter the parameters with which you want to execute the command. You can use the placeholders (variables) from section Parameters—Available Placeholders ³⁴⁶⁹ . Other placeholders are not possible. During runtime, these placeholders are replaced by the respective values set for the monitoring object you select to execute this device tool. For example, the %id placeholder will be replaced by the ID of a group, a device, or a sensor, depending on which object you execute the command for.
Shortcut	Select a key shortcut for the command. Choose an F -key from the list or select None to not use a key.

Parameters—Available Placeholders

The following placeholders (variables) are available in the Enterprise Console.

PLACEHOLDER	AVAILABLE FOR GROUPS	AVAILABLE FOR DEVICES	AVAILABLE FOR SENSORS	WILL BE RESOLVED TO
%id				The object's ID as shown in the page header on the object's details page
%name				The object's Name
%host				The sensor's or device's IP Address/DNS Name
%message				The sensor's Last Message
%value				The sensor's Last Result value
%type				The sensor's Type

If you use a placeholder in combination with an object it is not available for, it will simply not be resolved but the placeholder itself will be returned.

To see the output of all placeholders for different objects you can create a simple test tool that displays the output in a command line window. Just create a tool with the command **cmd** and the following content in the **Parameters** field:

```
/K echo.id: %id && echo.name: %name
    && echo.host: %host && echo.message: %message
    && echo.value: %value && echo.type: %type
```

Right-click an object in the device tree and run the tool from the **Tools** option in the menu (either [Windows](#)^[3472] or [context menu](#)^[3481]).

Select External Browser

From the [Windows menu](#)^[3472] of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

With these settings you can define which browser the Enterprise Console will use when you select a command that requires to open an external browser window, for example, when you select **View | Open in Web Browser** from the Windows menu of the EC. You can only select browsers installed on the system running the Enterprise Console, other browser options are disabled.

By default, the system's default browser is opened. To change the Enterprise Console's behavior, choose between:

- **Use system default browser** ([browser.exe](#))
- **Use IE (Version: x)**
 - ❗ Only Microsoft Internet Explorer 11 is supported by the Ajax web interface! Please do not use it with Internet Explorer 10 or earlier! We recommend that you use Google Chrome 67 or later (recommended) or Mozilla Firefox 61 or later as external browser.
- **Use Firefox (Version: x)**
- **Use Chrome (Version: x)**
- **Use Safari (Version: x)**

Proxy Settings

From the [Windows menu](#)³⁴⁷² of the Enterprise Console, select **File | Options...** to open the settings dialog. Please select a setting on the left and change the respective values on the right side. Click the **OK** button to save your settings.

If the connection to the PRTG core servers requires a proxy connection, you can set it here.

ENTERPRISE CONSOLE – OPTIONS: PROXY SETTINGS

No Proxy	Use a direct connection to the servers.
Use System Settings	Use your Windows default settings, configured in Internet Explorer . To view these settings, open the Internet Explorer on your system and select Tools Internet Options from the menu. Select the Connections tab and click the LAN settings button.
Manual Proxy Configuration	Manually enter a proxy configuration. Enter the IP address or DNS name of the proxy, a port number, as well as username and password (if required by the proxy). ❗ Only basic authentication is available!

Settings Storage

For each individual Windows user account, the settings of the Enterprise Console are stored in the Windows registry.

📖 For details, see section [Data Storage](#)³⁷³⁴.

9.6 Windows Menu Structure

The Windows menu of the Enterprise Console has four main menu items:

- [File](#)  3472
- [Edit](#)  3473
- [View](#)  3477
- [Help](#)  3478

File

The **File** menu offers system related options for the Enterprise Console. The particular close and exit options depend on the enabling status of the tray option.

FILE	
Manage PRTG Server Connections	<p>Show a list of all configured PRTG core server connections.</p> <p> For detailed instructions, see section PRTG Servers  3463 section.</p>
Options...	<p>Open the Options  3466 dialog to set EC system options and to configure one or more PRTG core server connections.</p>
Close or Exit	<p>This menu item appears as either Close or Exit, depending on whether the tray icon is enabled or disabled in the Options  3466 settings.</p> <ul style="list-style-type: none"> ▪ Use Close to close the Enterprise Console window. Alerting is still available via the tray icon then. You can also double-click the tray icon to re-open the Enterprise Console. ▪ Exit shuts down the Enterprise Console completely. This option is only available if the tray icon is not running. <p> Shortcut: Alt+X</p>
Close and Exit	<p>This menu item is only available if the Show in Tray option is enabled in the Options  3466 settings. It will completely shut down the Enterprise Console and tray icon, so no tray alerts are shown any more.</p> <p> Shortcut: Ctrl+Alt+X</p>

Edit

The content of the **Edit** menu varies, depending on which [menu tab](#)^[3438] you are and whether and which objects are selected within the [Devices](#)^[3439], [Sensors](#)^[3448], or [Alarms](#)^[3450] tab.

-  Some of the options open the Ajax web interface when you select them.
-  When you click one of these items, a new window or tab of the external browser configured in the Enterprise Console's [Options](#)^[3470] will open. PRTG automatically logs in and redirects you to the respective web page. If your browser displays a certificate warning, find more information in section [SSL Certificate Warning](#)^[172].

EDIT	
Scan Now	<p>Perform an immediate scan for all selected objects (use the Ctrl key to select multiple objects). This option polls all selected devices and queries new data for all sensors on them. If you choose this option for a probe or a group, you query data for all sensors in the object hierarchy^[133] underneath.</p> <p> Shortcut: Ctrl+K</p>
Details	<p>Open the overview tab for the selected object (probe, group, device, or sensor).</p>
Edit	<p>Access the pages for editing Settings...^[217], Notifications^[217], Access Rights...^[158], and Management^[217] (not for sensors) of the selected object. In addition, you can Rename... this object. Point on it to see available options.</p>
Dependencies	<p>This option is only available if you select a server (the Root group), a probe, or group. This function shows an overview of the dependencies^[141] configured for the selected object. If you select a dependencies option, the Enterprise Console opens the respective dependencies overview in a new window.</p> <p> For details, see section Show Dependencies^[320].</p>
Add Group...	<p>This option is only available if you select a probe or group (not the Root group). This option opens an assistant in a new window that guides you through adding a new group to the selected probe or group.</p> <p> For detailed instructions, see section Add a Group^[302].</p>
Add Auto-Discovery Group...	<p>This option is only available if you select a probe or group (not the Root group). This option opens an assistant in a new window that guides you through adding such a group.</p>

EDIT

 For detailed instruction, see section [Auto-Discovery](#) ^[282].

Add Device...

This option is only available if you select a probe or group (**not** the **Root** group). This option opens an assistant in a new window that guides you through adding a new device to the selected probe or group.

 For detailed instructions, see section [Add a Device](#) ^[311].

Add Sensor...

This option is only available if you select a device. This option opens an assistant in a new window that guides you through adding a new sensor to the selected device.

 For detailed instructions, see section [Add a Sensor](#) ^[325].

Auto-Discovery

This option is only available if you select a device. Hover over it to see available options. You can choose between:

- **Run Auto-Discovery**: This option starts an automatic search and adds new sensors to the selected device. The search is running in background. You will see new sensors after a few minutes automatically.

 If you have set the option **Manual (no auto-discovery)** in the [device settings section](#) ^[404] **Sensor Management** and start the auto-discovery, PRTG will not run it. Please note that the [Ajax web interface](#) ^[254] behaves differently in this case.

- **Run Auto-Discovery with Template**: With this option you can run an auto-discovery with a pre-defined device template.

 For more information, see section [Auto-Discovery](#) ^[283] (**Run Auto-Discovery Now**).

Create Device Template...

This option is only available if you select a device. This option opens an assistant in a new window that guides you through creating a device template. This template is then available for [auto-discovery](#) ^[282].

 For detailed instructions, see [Create Device Template](#) ^[3203].

Sort Alphabetically

This option is only available if you select a probe, a single group, or a device. This will sort direct children of the selected node such as groups, devices, or sensors in alphabetical order.

 The ordering is stored in the monitoring configuration so you cannot revoke it!

EDIT

- Acknowledge Alarm...** This option is only available if you select a sensor in a **Down** or **Down (Partial)** [status](#)¹⁹⁵. Point on it to see available options.
-  For details on how to acknowledge an alarm, see section [Alarms](#)³⁴⁵¹.
- Delete** Delete the selected object(s). You will be asked for confirmation before anything is actually deleted.
- Clone...** This option is only available if you select a single group, device, or sensor. This options opens an assistant in a new window that guides you through cloning the selected object.
-  For detailed instructions, see section [Clone Object](#)³¹⁹³.
- Move** Move the selected object(s) of the device tree (use the **Ctrl** or **Shift** key to select multiple objects). Hover over it to see available options. Choose between **Top**, **Up**, **Down**, and **Bottom** to move the object(s) to the top or bottom of the mother node, or one entry up or down.
- You can also move the selected group or device to another group with **To Other Group...** This option opens an assistant in a new window to guide you through the movement.
-  For details about allowed movements, see section [Devices](#)³⁴⁴⁵.
- Pause** Pause and resume monitoring for the selected objects from the device tree (use the **Ctrl** key to select multiple objects). Hover over it to see available options.
- Choose between:
- **Indefinitely**
 - **Resume**
 - **For 5 Minutes**
 - **For 15 Minutes**
 - **For 1 Hour**
 - **For 3 Hours**
 - **For 1 Day**

EDIT

- **Pause Until...:** This option will open an assistant in a new window where you can enter a message and a date. Use the date time picker to enter the date and time. PRTG will resume monitoring after this date.

You can also set up a **One-time maintenance window**: Enter a message and start and end date of the maintenance in the appearing window. Use the date time picker to enter the date and time.

Simulate Error Status

This option is only available if you select a sensor. Set the selected sensor to a simulated error status. As for the pause status, **Resume** will appear in the context menu if a the selected sensor is already in a simulated error state.

- ❗ **Simulate error status** does not work for sensors that run on a PRTG Mini Probe.

Priority/Favorite

Set the priority for the selected object. You can also add devices and sensors to favorites.

- 📖 For details, see section [Priority and Favorites](#) ²⁴².

Historic Data

Open the historic data tab of the selected object. Hover over it to see available options.

You can choose between **Last 2 days...**, **Last 30 days...**, and **Last 365 days....**, or when selected one sensor **Live Data...** and **View Historic Data....** You can also create a report.

- 📖 For detailed instructions, see [Historic Data Reports](#) ²⁰⁵ (Menu).

When you select one or more sensors (hold the **Ctrl** or **Shift** key to select multiple items), you can open the **Compare Sensors** dialog. The graphs of all chosen sensors appear in the comparison dialog automatically. You can add additional sensors in the comparison dialog.

- For sensors, you can open the [Similar Sensors Overview](#) ²⁰⁹.

Device Tools

Call a tool command. All placeholders (variables) configured in a tool command will be resolved for the currently selected object. Hover over it to see all available tools configured in your [Options](#) ³⁴⁶⁸ settings (**Device Tools**).

By default, a **Remote Desktop** tool is pre-configured that tries to initiate a remote desktop connection to the IP address or DNS name of the selected object. This will usually work for devices.

EDIT

You can also add a device tool directly to the selected object: **Add Device Tool...** will open [Options—Device Tools](#)³⁴⁶⁸.

For devices, additional options are available. They allow you to connect to the **Service URL** value defined in the device's [settings](#)³⁴⁴⁴, or open the **IP address/DNS name** of the device via the protocols **HTTP**, **HTTPS**, and **FTP**. For each of these functions, your system's default programs will be used. Usually, this is your browser. You can also install a remote probe on a device via [Remote Probe Quick Setup](#)³⁷¹³.



You may need to run the Enterprise Console as administrator to make the tool function work with your Windows version.

Find Duplicates

This option is only available if you select a device. Search in your PRTG configuration for devices with the same IP address or DNS name as the selected device. A new window with the results will appear, either showing existing duplicates or a message indicating that there are no duplicates.

Drag & Drop Sorting

Enable this option to sort all objects in the device tree via drag and drop. By default, this option is disabled to avoid accidental moves of objects.



For details, see section [Devices](#)³⁴⁴⁶.

Send Link by Email

Send the link to the selected object by email. This option opens a new email using your system's standard email client. It contains a direct link to the details page of the selected object.

Open Ticket

Open a ticket that refers to the currently selected object.



For details, see section [Tickets](#)³⁴⁵⁸.

Open in Web Browser

Open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. You can set the default browser in the [Options](#)³⁴⁷⁰ settings.

View

The **View** menu provides settings related to what the Enterprise Console shows.

VIEW

Refresh	<p>Query data for the current screen from the PRTG core server immediately, just as the automatic refresh does. You can configure the auto-refresh in the Options³⁴⁶⁶ settings.</p> <p> Shortcut: F5</p>
Large Single Graph	<p>Change the view in Devices³⁴³⁹ menu tabs to large single graphs. This option displays live graphs and graphs for three other time spans in different tabs.</p> <p> Shortcut: Ctrl+L</p>
Small Multiple Graphs	<p>Change the view in Devices³⁴³⁹ menu tab to multiple small graphs. This option displays live graphs and graphs for three other time spans in one tab.</p>
Show Geo Maps	<p>Choose if you want to show Geo Maps³²¹¹ in the Enterprise Console.</p> <p> Shortcut: Ctrl+G</p>
Show News Feed	<p>Choose if you want to show the news feed in the Enterprise Console.</p> <p> Shortcut: Ctrl+N</p>
Next Viewpoint	<p>Go forward to the next viewpoint (only available if you went back to a previous viewpoint before). This is similar to a browser's function to go forth in history.</p> <p> Shortcut: Alt+Right</p>
Previous Viewpoint	<p>Go backwards to the previous viewpoint. This is similar to a browser's function to go back in history.</p> <p> Shortcut: Alt+Left</p>
Open in Web Browser	<p>Open the currently selected object in the Ajax web interface. This option is not available if multiple objects are selected. You can set the default browser in the Options³⁴⁷⁰ settings.</p>

Help

This menu provides links to help and information.

HELP

Help Center	Open the Help and Support Center in the Ajax web interface.
HTML Manual Enterprise Console...	Open the Enterprise Console ³⁴³⁰ sections of this manual in the Ajax web interface.
PRTG Network Monitor Homepage...	Open https://www.paessler.com/prtg in your browser for overall information about PRTG.
Contact Support	Open the Contact Support ³⁴²⁴ dialog box to leave feedback or to ask for support by sending a support bundle.
About...	Open an information window about the Enterprise Console application with version number and copyright information.

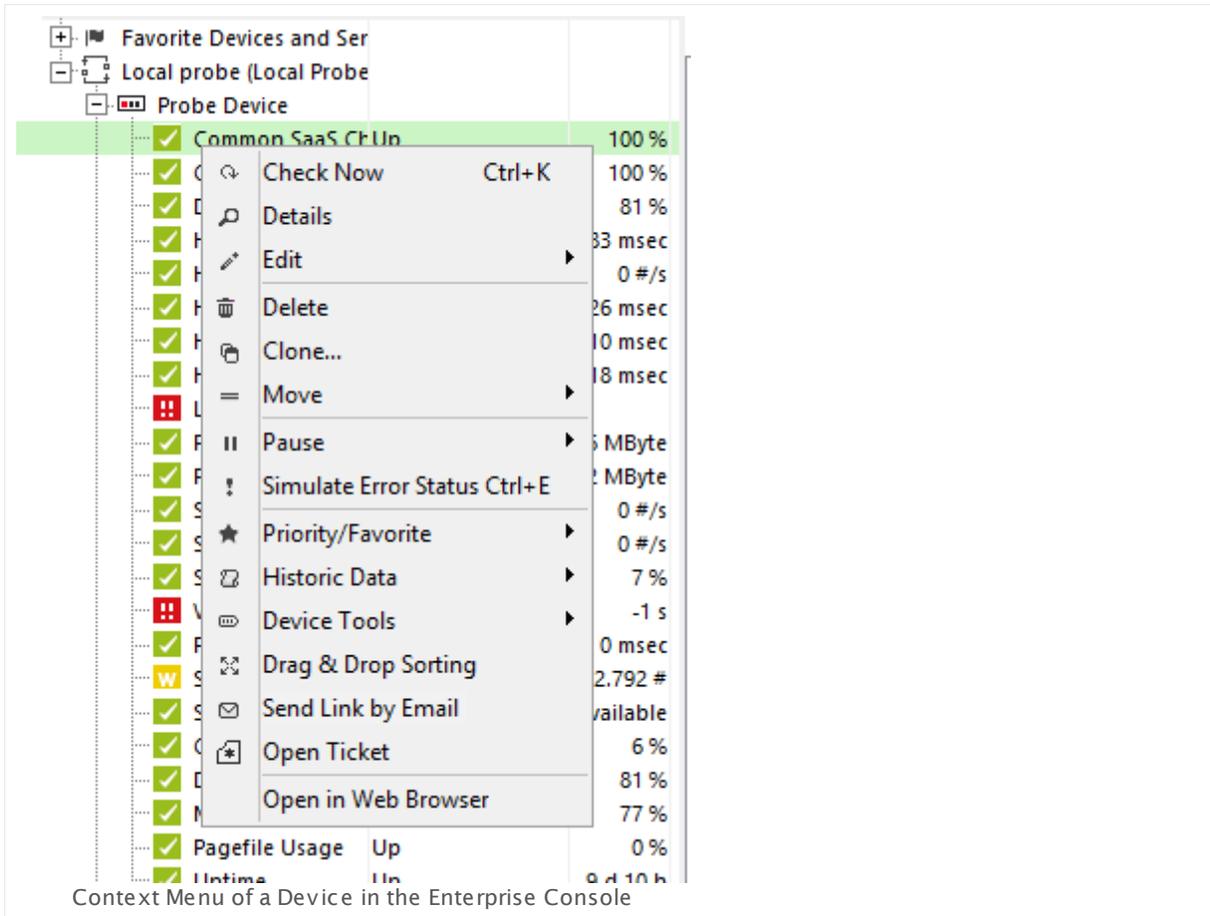
See Also

- [Shortcuts Overview](#)³⁴⁵¹

9.7 Context Menus

For every object in the Enterprise Console, there are context menus available that appear when you right-click an object in the device tree. These context menus vary depending on the selected object and always contain a sub-set of the options available in the Windows menu.

For detailed explanations, see section [Windows Menu Structure](#) ³⁴⁷².



9.8 Shortcuts Overview

The following shortcut keys are available in the Enterprise Console:

- **Alt+X**: File | Close **or** Exit
With the **Show in Tray** option enabled in the [Options](#)³⁴⁶⁶ settings, this is **Close**, otherwise **Exit**.
- **Ctrl+Alt+X**: File | Close and Exit
This menu item is only shown if the **Show in Tray** option is enabled in the [Options](#)³⁴⁶⁶ settings.
- **Alt+Right**: Next Viewpoint
- **Alt+Left**: Previous Viewpoint
- **Ctrl+K**: Edit | Scan Now
- **Ctrl+P**: Edit | Pause | Indefinitely
- **Ctrl+R**: Edit | Pause | Resume
- **Ctrl+E**: Edit | Simulate Error Status
- **Ctrl+L**: View | Large Single Graph
- **Ctrl+S**: View | Small Multi Graphs
- **Ctrl+G**: View | Show Geo Maps
- **Ctrl+N**: View | Show News Feed
- **F5**: View | Refresh
- **F6**: [Context Menu] | Tools | **Custom tool command, if available**
- **F7**: [Context Menu] | Tools | **Custom tool command, if available**
- **F8**: [Context Menu] | Tools | **Custom tool command, if available**
- **F9**: [Context Menu] | Tools | **Custom tool command** (default: **Remote Desktop**)
- **F10**: [Context Menu] | Tools | **Custom tool command, if available**
- **F11**: [Context Menu] | Tools | **Custom tool command, if available**
- **F12**: [Context Menu] | Tools | **Custom tool command, if available**

See Also

- [Windows Menu Structure](#)³⁴⁷²

Part 10

PRTG Apps for Mobile Network Monitoring

10 PRTG Apps for Mobile Network Monitoring

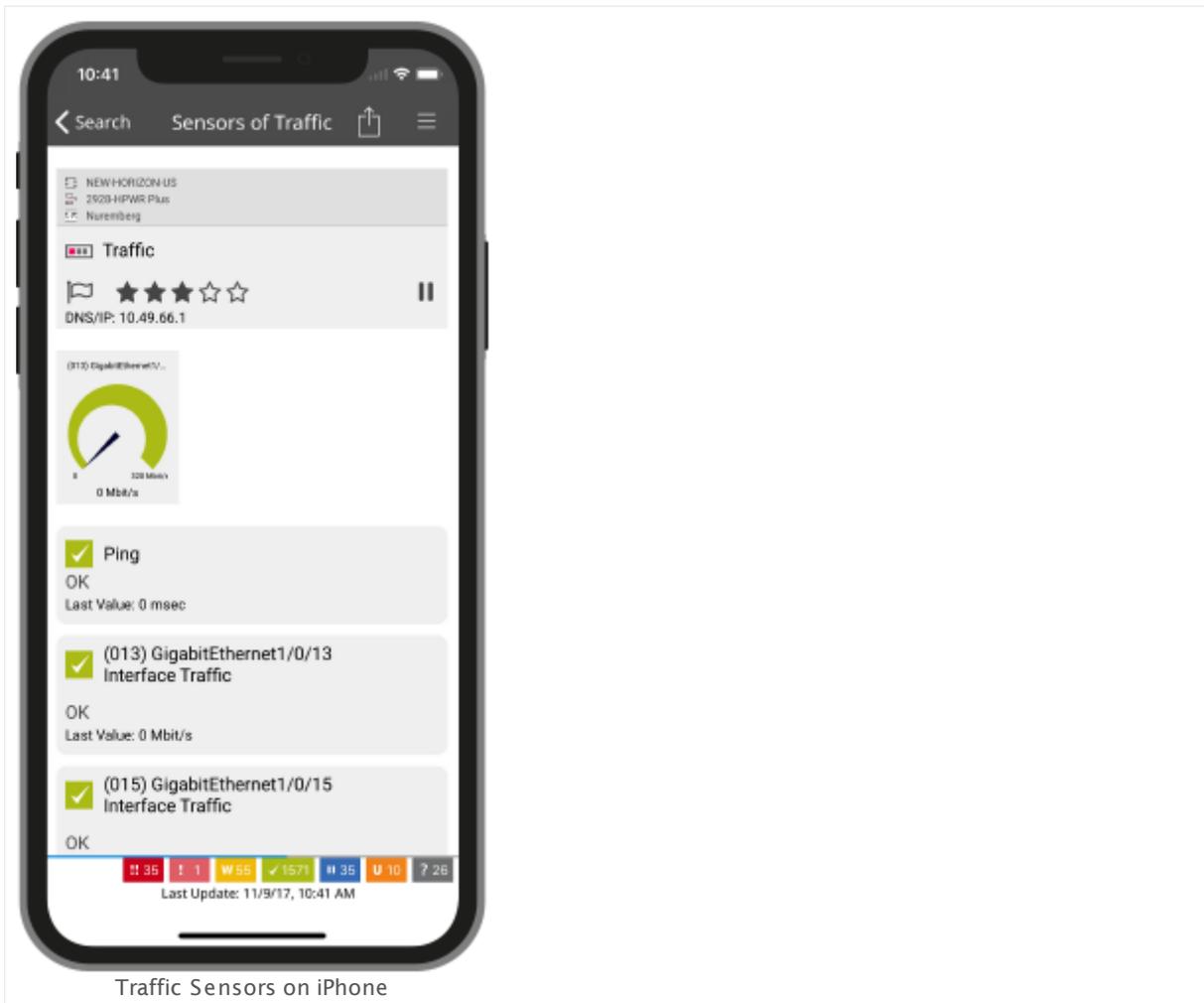
You can access your PRTG installation on your mobile devices with several PRTG apps. We provide apps for iOS devices and Android systems. You can download and use these apps for free. [PRTG for iOS](#)³⁴⁸⁴ and [PRTG for Android](#)³⁴⁸⁵ make it possible to monitor your network while on the go.

The basic requirements to use these free apps are a running PRTG core server that is accessible from the network your device is connected to (either directly or via a VPN connection) and a recent operating system version on your mobile device. For details about requirements, see below.

PRTG for iOS

PRTG for iOS is the iOS app for PRTG Network Monitor version 13 or later. You can use the newest app version on iPhone, iPad, and iPod touch with iOS version 9 or later. You can also use free [push notifications](#)³³¹⁹ with this app (required: PRTG for iOS 14.3.6 or later; PRTG 15.4.20 or later).

 For more information and to download this app, see our website: [PRTG for iOS](#).



Traffic Sensors on iPhone

PRTG for Android

PRTG for Android is the Android app for PRTG Network Monitor version 14 or later. Use it on your smartphone or tablet with Android version 4.0 or later, or on a Kindle Fire. For full functionality, we recommend that you use at least Android 4.1. You can also use free [push notifications](#) with the PRTG for Android app (required: PRTG for Android 14.3.2 or later; PRTG 15.4.20 or later).

 For more information and to download this app, see our website: [PRTG for Android](#)



Sensor List on PRTG
for Android

More

PRTG for iOS:

- <https://www.paessler.com/apps/iosapp>

PRTG for Android:

- <https://www.paessler.com/apps/androidapp>

Knowledge Base: Which features do the PRTG mobile apps support?

- <https://kb.paessler.com/en/topic/60042>

Knowledge Base: How can I use push notifications with PRTG?

- <https://kb.paessler.com/en/topic/60892>

Part 11

Sensor Technologies

11 Sensor Technologies

This section introduces different technologies that PRTG uses for monitoring to give you more background information. Please read more in the following sections.

Sensor Technologies—Topics

- [Monitoring via SNMP](#)  3489
- [Choosing the Right SNMP Sensor](#)  3494
- [Monitoring via WMI](#)  3507
- [Monitoring via SSH](#)  3510
- [Monitoring Bandwidth via Packet Sniffing](#)  3512
- [Monitoring Bandwidth via Flows](#)  3514
- [Bandwidth Monitoring Comparison](#)  3517
- [Monitoring Quality of Service](#)  3519
- [Monitoring Email Round Trip](#)  3524
- [Monitoring Backups](#)  3526
- [Monitoring Virtual Environments](#)  3527
- [Monitoring Databases](#)  3534
- [Monitoring Syslogs and SNMP Traps](#)  3539
- [Monitoring via Push](#)  3548
- [Monitoring via HTTP](#)  3552

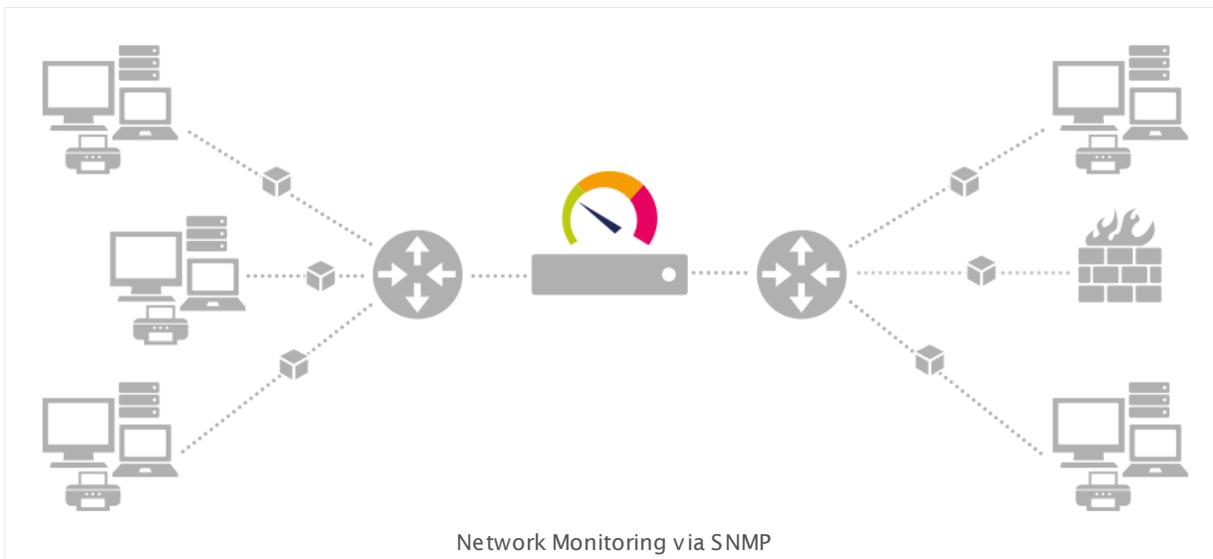
11.1 Monitoring via SNMP

Monitoring via Simple Network Management Protocol (SNMP) is the most basic method of gathering bandwidth and network usage data.

How SNMP Monitoring Works

SNMP is a set of standards for communication with devices in a TCP/IP network. SNMP monitoring is useful if you are responsible for servers and network devices such as hosts, routers, hubs, and switches. It enables you to keep an eye on network and bandwidth usage, and monitor important issues such as uptime and traffic levels.

You can use SNMP to monitor the bandwidth usage of routers and switches on a port-by-port basis, as well as device readings such as memory and CPU load. The target devices must support SNMP. Most devices with enabled SNMP require the same configuration like SNMP version and community string. To find out how to set up SNMP on a specific device, search in the internet for your device name or model and SNMP configuration. You will likely get plenty of information on how to configure SNMP.



When you use a sensor with this technology, PRTG sends small data packets to devices, for example, querying routers, switches, and servers for the traffic counters of each port. These queries trigger reply packets from the device. Compared to PRTG's other bandwidth monitoring technologies via flows, packet sniffing, or WMI, the SNMP option creates the least CPU and network load.

Reasons to Choose SNMP Monitoring

SNMP is the most commonly used method mainly because it is easy to set up and requires minimal bandwidth and CPU cycles. If your network devices support SNMP and/or if you want to monitor large networks with several hundred or thousands of sensors, we recommend that you start with SNMP.

Besides network usage monitoring, another well-known feature of SNMP is the ability to also watch other network parameters such as CPU load, disk usage, temperature, as well as monitoring many other readings, depending on the queried device.

SNMP Network Issues

To use Simple Network Management Protocol (SNMP) for monitoring purposes, it is imperative that UDP packets can travel from the machine running PRTG to the device you want to monitor and back. This is usually the case in LANs and intranets. For connections across the internet, to a Demilitarized Zone (DMZ), or for Wide Area Network (WAN) connections, some changes to the traversed firewalls may be necessary.

Keep in mind that SNMP V1 and V2c are not secure protocols so you should not use them across the internet or insecure data connections. Only SNMP version 3 supports encryption.

Understanding SNMP Sensors

To better understand and set up SNMP sensors, you may want to learn more about the principles of [Object Identifiers \(OID\)](#) and [Management Information Base \(MIB\)](#).

-  For more information about this topic, see this Knowledge Base article: [How do SNMP, MIBs and OIDs work?](#)
-  For an overview and details about all SNMP sensors, see section [List of Available Sensor Types](#)^[431].
-  For more information about which SNMP sensor is best for your monitoring setup, see section [Choosing the Right SNMP Sensor](#)^[3494].

SNMP Versions

PRTG supports three versions of the SNMP protocol: Version 1, version 2c, and version 3.

SNMP Version 1

This is the oldest and most basic version of SNMP.

- Pro: Supported by most SNMP-compatible devices; simple to set up.
- Con: Limited security because it only uses a simple password ([community string](#)^[3492]) and sends data in clear text (unencrypted). Because of this, you should only use it inside LANs behind firewalls, but not in WANs. Version 1 only supports 32-bit counters, which are not enough for high-load (gigabits/second) bandwidth monitoring.

SNMP Version 2c

This version adds 64-bit counters.

- Pro: Supports 64-bit counters to monitor bandwidth usage in networks with gigabits/second loads.

- Con: Limited security (same as with SNMP V1).

SNMP Version 3

This version adds authentication and encryption to SNMP.

- Pro: Offers user accounts and authentication for multiple users and optional data packet encryption, increasing available security; plus all advantages of Version 2c.
- Con: Difficult to configure and higher overhead for the probe, which will reduce the number of devices that you can monitor (see [here](#)³⁴⁹¹ for more information).

SNMP Traps

Various devices can send SNMP trap messages to notify you of system events.

- PRTG supports SNMP v1 and SNMP v2c traps.
- Destination for SNMP traps: IP address of the trap receiver, which is the IP of the PRTG probe system (server with either a local or remote probe running on it) to which you add the [SNMP Trap Receiver Sensor](#)²⁴⁷⁹.

Which SNMP Version Should I Choose?

The SNMP version to choose depends on your environment, but as a guideline:

- If your network is publicly accessible, you may want to use SNMP v3, which has encryption and secure access. However security and encryption adds overhead, which results in less performance.
- If your network is isolated or well protected behind firewalls, the lower security of SNMP v1 or SNMP v2c may be sufficient.
- From the PRTG perspective, if you have a lot of devices to monitor, the SNMP v2c is preferable. It will allow you to monitor more devices on a shorter monitoring interval and supports 64-bit counters.

The most important thing is to set the same SNMP version in the PRTG settings (for example, on **Root** level) as you have configured in your target device. If you select an SNMP version that is not supported by the server or device you want to monitor, you receive an error message. Unfortunately, in most cases, these error messages do not explicitly point to the possibility that you use the incorrect SNMP version. These messages provide minimum information only, such as **cannot connect** or similar. Similar errors occur when community strings, usernames, or passwords do not match.

 For basic requirements for SNMP monitoring, see this Knowledge Base article: [My SNMP sensors don't work. What can I do?](#)

SNMP Overload and Limitations of the SNMP System

SNMP V1 and V2 scale directly with the performance of the hardware and the speed of the network. In our labs we are able to monitor 30,000 SNMP V1 sensors at a 60 second interval with one PRTG server (core and local probe) plus two remote probes with 10,000 sensors each.

However, SNMP V3 has performance limitations due to the SSL encryption. The main limiting factor is CPU power (as well as the other general limits for PRTG). Because of this limitation, you can monitor only a limited number of sensors per second using SNMP V3. Currently, PRTG is able to handle about 40 requests per second and computer core, depending on your system. This means that, on a common 1.x GHz computer with two cores, you can run about 5,000 SNMP v3 sensors with a 60 seconds scanning interval; on a system with four cores, you can monitor around 10,000 sensors with 60 seconds interval. The CPU load is at about 50% then. We do not recommend more.

Furthermore, the PRTG core server and probes should run on different computers. If you experience increased values in the **Interval Delay SNMP** or **Open Requests** channels of the **Probe Health Sensor** (values above 0 % indicate that the SNMP requests cannot be performed at the desired interval), you need to distribute the load over multiple probes. SNMP V1 and V2 do not have this limitation.

If you run into SNMP overload problems, you have three options:

- Increase the monitoring interval of the SNMP V3 sensors.
- Distribute the SNMP V3 sensors over two or more probes.
- Switch to SNMP V1 or V2 if you can go without encryption.

What is the SNMP Community String?

The SNMP **Community String** is similar to a user ID or password that allows access to the statistics of a router or another device. PRTG Network Monitor sends the community string along with all SNMP requests. If the correct community string is provided, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

i SNMP community strings are only used by devices that support SNMP V1 and SNMP V2c protocols. SNMP V3 uses safer username/password authentication, along with an encryption key.

By convention, most SNMP V1/V2c equipment ships with a read-only community string set to the value **public**. It is standard practice for network managers to change all the community strings to customized values during device setup.

More

Tools: Paessler MIB Importer and SNMP Tester

- <https://www.paessler.com/tools/>

Knowledge Base: How do SNMP, MIBs and OIDs work?

- <https://kb.paessler.com/en/topic/653>

Paessler White Papers: **Introducing SNMP** and **Putting SNMP into Practice**

- https://www.paessler.com/press/whitepapers/introducing_snmp

German: Paessler White Paper: **Einführung in SNMP** und **SNMP praktisch anwenden**

- http://www.de.paessler.com/press/whitepapers/introducing_snmp

Video Tutorial: SNMP Basics

- <https://www.paessler.com/support/videos/prtg-basics/snmp-basics>

Video Tutorial: Debugging SNMP

- <https://www.paessler.com/support/videos/prtg-basics/snmp-debugging>

Knowledge Base: My SNMP sensors don't work. What can I do?

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: The interface numbers on my switch keep changing. What can I do?

- <https://kb.paessler.com/en/topic/62217>

Knowledge Base: What can I check if SNMP and SSH sensors throw timeout and auth errors?

- <https://kb.paessler.com/en/topic/63794>

Knowledge Base: What can I monitor with the SNMP Custom Table sensor?

- <https://kb.paessler.com/en/topic/68539>

11.1.1 Choosing the Right SNMP Sensor

The Simple Network Management Protocol (SNMP) is easy to use and generally requires little configuration once it is set up. Many network devices support it and many parameters can be monitored with it. So to help cover all of your monitoring needs, PRTG provides you with around 70 SNMP sensors. These sensors range from monitoring general parameters to very specific parameters. Choosing the right sensor for SNMP monitoring that gives you the desired hardware parameters is a decision that depends on several factors: the type of hardware you have, what values you want to monitor, and a few others.

Check SNMP Capability

Make sure that each device you want to monitor supports SNMP, and that it is enabled. You can find out whether SNMP is supported by a device by either going to the vendor's website or check that it is enabled in the configuration of the device.

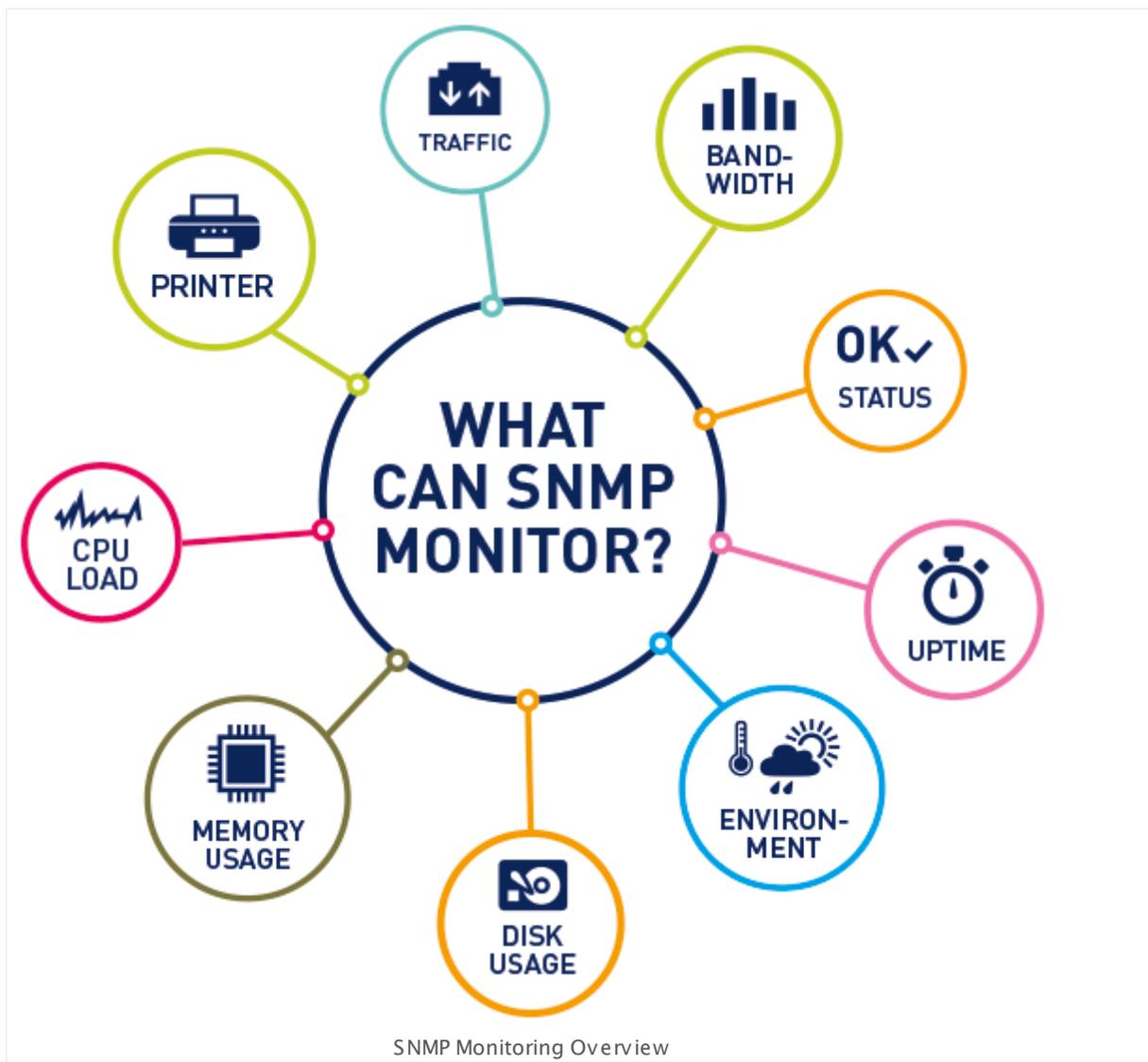
 If you are uncertain whether SNMP is enabled on the target device and works, we recommend that you try our [SNMP Tester](#), designed for just this purpose. You can scan for uptime to perform a basic check for SNMP availability of the target device.

Setup Checklist

1. Enable SNMP on the device.
2. Allow access to SNMP for the machine running PRTG Network Monitor in the device's security settings.
3. Allow User Datagram Protocol (UDP) packages to travel from the machine running PRTG to the device you want to monitor and back.
4. SNMP requires the use of UDP ports >1023 to the PRTG client side. This is important for your firewall settings.
5. Ensure that the firmware of the monitored device is up to date.
6. Select the appropriate SNMP protocol.

 It is important to know which SNMP version you have to select, because if it is not supported by the server or device you want to monitor, you will receive an error message.

 See this article in our Knowledge Base for more information: [General Introduction to SNMP and PRTG](#)



Vendor Specific SNMP Sensors

PRTG offers many vendor specific SNMP sensors for some common vendors. These sensors have been tailored to fit the end devices perfectly. Many years of experience allow us to work around familiar vendor implementation errors, for example if SNMP has not been fully implemented on an end device according to the RFCs. In this case, our vendor specific sensors still automatically receive the most important values with little to no effort on your part (looking for Object Identifiers (OIDs), for example). These sensors take care of everything for you.

Supported Vendors

- APC
- Buffalo
- Cisco

Part 11: Sensor Technologies | 1 Monitoring via SNMP

1 Choosing the Right SNMP Sensor

- Dell
- Fujitsu
- HP
- IBM
- Jakarta
- Juniper
- LenovoEMC
- NetApp
- Poseidon
- QNAP
- SonicWall
- Synology



For more information, see this article in our Knowledge Base: [What SNMP Sensors does PRTG offer?](#)

Generic SNMP Sensors

PRTG offers several generic sensors that work with practically any device that supports SNMP, the corresponding Management Information Base (MIB) and Object Identifiers (OIDs), and correctly implements the according RFCs. The standard SNMP libraries of PRTG include predefined, common values for the generic SNMP sensors so that you can easily get started with monitoring via SNMP. You can monitor the following parameters with the generic sensors.

SENSOR	WHAT IT MONITORS
SNMP CPU Load sensor <small>1941</small>	<p>The SNMP CPU Load sensor monitors the system load using Simple Network Management Protocol (SNMP).</p> <ul style="list-style-type: none">▪ It shows the load of several CPUs in percent.
SNMP Disk Free sensor <small>2507</small>	<p>The SNMP Disk Free sensor monitors the free disk space on a logical disk via Simple Network Management Protocol (SNMP).</p> <p>It can show the following:</p> <ul style="list-style-type: none">▪ Free disk space in percent▪ Free disk space in bytes▪ Total disk space

SENSOR	WHAT IT MONITORS
SNMP Hardware Status sensor <small>2082</small>	<p>The SNMP Hardware Status sensor monitors the status of a hardware component of a server via Simple Network Management Protocol (SNMP).</p> <p>It shows the following:</p> <ul style="list-style-type: none">▪ Current status of the monitored hardware component▪ Number of errors per time period
SNMP Memory sensor <small>2288</small>	<p>The SNMP Memory sensor monitors the memory usage of a system via Simple Network Management Protocol (SNMP).</p> <p>It can show the following:</p> <ul style="list-style-type: none">▪ Available memory in bytes▪ Available memory in percent▪ Total memory
SNMP Printer sensor <small>2370</small>	<p>The SNMP Printer sensor is a generic sensor that monitors various types of printers via Simple Network Management Protocol (SNMP).</p> <p>It can show the following:</p> <ul style="list-style-type: none">▪ Total number of printed pages▪ Fill level of cartridges and toners▪ Status of the printer cover▪ Additionally, the sensor shows the printer status as sensor message.
SNMP RMON sensor <small>2403</small>	<p>The SNMP RMON sensor monitors traffic on a device using the Remote Monitoring (RMON) standard via Simple Network Management Protocol (SNMP). You can create it on an SNMP compatible device that provides traffic data via RMON. Depending on the data returned by your device, traffic data for each port can be displayed in different channels, allowing detailed analysis. If available, the sensor queries 64-bit counters.</p> <p>For each port, the sensor can show, for example:</p> <ul style="list-style-type: none">▪ Transmitted kbit/s▪ Packets (#/s)

SENSOR

WHAT IT MONITORS

- Broadcast Packets (#/s)
- Multicast Packets (#/s)
- CRC Errors (#/s)
- Undersize Packets (#/s)
- Oversize Packets (#/s)
- Fragments (#/s)
- Jabbers (#/s)
- Collisions (#/s)
- Packets <= 64 Byte (#/s)
- Packets 65 - 127 Bytes (#/s)
- Packets 128 - 255 Bytes (#/s)
- Packets 256 - 511 Bytes (#/s)
- Packets 512 - 1023 Bytes (#/s)
- Packets 1024 - 1518 Bytes (#/s)
- Drop Events (#/s)

[SNMP System Uptime sensor](#)

The SNMP System Uptime sensor monitors the time a device is running via Simple Network Management Protocol (SNMP).

- It reads the system uptime value of the monitored device and shows it.

[SNMP Traffic sensor](#)

The SNMP Traffic sensor monitors traffic on a device using Simple Network Management Protocol (SNMP). You can create it on a device that provides traffic data, one traffic sensor for each individual port.

It can show the following:

- Traffic in
- Traffic out
- Traffic total

You can also add additional channels:

- Errors in and out
- Discards in and out

SENSOR	WHAT IT MONITORS
SNMP Trap Receiver sensor <small>2479</small>	<ul style="list-style-type: none">▪ Unicast packets in and out▪ Non unicast packets in and out▪ Multicast packets in and out▪ Broadcast packets in and out▪ Unknown protocols <p>The SNMP Trap Receiver sensor receives and analyzes Simple Network Management Protocol (SNMP) traps.</p> <p>It shows the following:</p> <ul style="list-style-type: none">▪ Overall number of received traps per second▪ Trap messages categorized as "warning" per second▪ Trap messages categorized as "error" per second▪ Number of dropped trap packets per second▪ The actual trap messages

Operating System-based SNMP Sensors

PRTG also offers several operating system-based SNMP sensors that extend your SNMP monitoring. You can monitor the following parameters with these sensors.

SENSOR	WHAT IT MONITORS
SNMP Linux Disk Free sensor <small>2251</small>	<p>The SNMP Linux Disk Free sensor monitors free space on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).</p> <p>It shows the following:</p> <ul style="list-style-type: none">▪ Free total disk space in bytes▪ Free space in bytes for every mounted partition▪ Free space in percent for every mounted partition▪ Free inodes in percent for every mounted partition

SENSOR

WHAT IT MONITORS

[SNMP Linux Load Average sensor](#) 2263

The SNMP Linux Load Average sensor monitors the system load average of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Average system load within a 1-minute interval
- Average system load within a 5-minute interval
- Average system load within a 15-minute interval

[SNMP Linux Meminfo sensor](#) 2271

The SNMP Linux Meminfo sensor monitors the memory usage of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following :

- Available memory in absolute and percentage values
- Used physical memory (free memory plus buffer plus cache) in percent
- Free physical memory (free memory plus buffer plus cache) in bytes
- Used swap memory in percent
- Free swap memory in bytes
- Used memory on the whole system (physical memory plus swap) in percent
- Free memory on the whole system (physical memory plus swap) in bytes

[SNMP Linux Physical Disk sensor](#) 2273

The SNMP Linux Physical Disk sensor monitors input/output (I/O) on disks of a Linux/Unix system using Simple Network Management Protocol (SNMP).

It shows the following:

- Read bytes per second
- Written bytes per second
- Number of read accesses per second
- Number of write accesses per second

SENSOR	WHAT IT MONITORS
SNMP Windows Service sensor  2492	<p>The SNMP Windows Service sensor monitors a Windows service via Simple Network Management Protocol (SNMP).</p> <ul style="list-style-type: none"> ▪ It shows the operating status of the monitored service.

Custom SNMP Sensors

For your more individual needs, PRTG offers custom SNMP sensors. The monitoring capabilities of these sensors go beyond the scope of the generic sensors. The custom sensors allow you to show certain values that are not included in the standard libraries of PRTG. With these sensor types, you can monitor most devices that support SNMP and that PRTG does not have native sensor types for. Basically, you just need to find out the required Object Identifiers (OIDs) for your desired device readings, for example, in the vendor's documentation of your hardware device.

 For more details, see the Knowledge Base: [How do I find out which OID I need for an SNMP Custom sensor?](#)

SENSOR	WHAT IT MONITORS
SNMP Custom sensor  1949	<p>The SNMP Custom sensor monitors a single parameter that is returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP).</p> <ul style="list-style-type: none"> ▪ This sensor shows a single numerical value (int64) for a given OID. Each OID always refers to a specific parameter of a certain SNMP device. <p>Value types include the expected numeric type of the results at the given OID: You can choose between</p> <ul style="list-style-type: none"> ▪ Absolute (unsigned integer): for integer values such as 10 or 120 ▪ Absolute (signed integer): for integer values such as -12 or 120 (negative values supported) ▪ Absolute (float): for float values such as -5.80 or 8.23 (with decimal places) ▪ Delta (counter): PRTG calculates the difference between the previous and the current value. <p> See this video tutorial SNMP Custom and Library Sensor on our website for more information.</p>

SENSOR

WHAT IT MONITORS

[SNMP Custom Advanced sensor](#) 

The SNMP Custom Advanced sensor monitors numerical values returned for Object Identifiers (OIDs) using Simple Network Management Protocol (SNMP).

- The sensor displays numerical values for given OIDs that refer to this specific SNMP device. Up to 10 OIDs and corresponding numerical values are possible.

This sensor monitors very similarly to the regular SNMP Custom sensor, with the advantage of being able to poll up to 10 specific OIDs with a single sensor. For each OID you will be able to define a name, OID, expected type, and the unit to be displayed. The possible value types are the same as with the SNMP Custom sensor.

[SNMP Custom String sensor](#) 

The SNMP Custom String sensor monitors a string returned by a specific Object Identifier (OID) using Simple Network Management Protocol (SNMP). It can check for keywords. If you want to set limits to the sensor channel value, you can also extract a numeric value contained in the string.

This sensor shows the following:

- Response time of the monitored device
- Optionally a value extracted from the string
- In the sensor message, the sensor shows the string you [search](#)  for and which is the reason for a current **Warning** or **Down status** .

Hexadecimal-encoded strings can also be decoded as MAC addresses or IP addresses. The sensor can check for keywords via plain text or regular expression or you can use a regular expression to extract a numerical value from the string that can be evaluated later for additional alerts.

- See section [Number Extraction with Regular Expression](#)  for an example.

SENSOR

WHAT IT MONITORS

[SNMP Custom String Lookup sensor](#)

The SNMP Custom String Lookup sensor monitors a string that a specific Object Identifier (OID) returns via Simple Network Management Protocol (SNMP). It can map the string directly to a [sensor status](#) by using a [defined lookup file](#). Basically, this sensor type does a "reverse lookup". You have to define all potential return strings in the lookup file as text values, each in one lookup entry. Graphs and data tables show the value to which the string is mapped, usually an integer ([lookup type](#) **SingleInt**). See manual section [SNMP Custom String Lookup Sensor—Example](#).

- This sensor shows a retrieved string value and its status, as defined in the corresponding lookup file.

[SNMP Custom Table sensor](#)

The SNMP Custom Table sensor monitors entries from a table that is provided via Simple Network Management Protocol (SNMP). You can create one new sensor per table row. For each sensor, you can define up to ten channels. Each channel shows the value of one defined table column.

- It can show numerical values in up to 10 channels per table row.

Vendors use tables when there are multiple instances of the same object (for example, memory, disks). The sensor recognizes a table via a meta-scan and allows you to configure the indexes (interfaces) that you want to monitor.

 For more details, see the Knowledge Base: [What can I monitor with the SNMP Custom Table Sensor?](#)

[SNMP Library sensor](#)

The SNMP Library sensor uses a compiled Management Information Base (MIB) library file to create sensors that monitor a device via Simple Network Management Protocol (SNMP). This approach provides custom monitoring beyond the standard SNMP sensors of PRTG.

The content of the MIB file will determine which data types are available for monitoring. When you create the sensor, it will provide a list of counters that came back from the target device based on checking every Object Identifier (OID) in the MIB. From this list, you can choose what you want to monitor.

The SNMP Library sensor will automatically create the following custom SNMP sensor types based on the data types available in the MIB:

- [SNMP Custom Advanced sensors](#) for all OIDs the return single values

SENSOR

WHAT IT MONITORS

- [SNMP Custom String sensors](#)  for all OIDs that return string values
- [SNMP Custom Table sensors](#)  for all OIDs that return tables

 The SNMP Library sensor is not actually a sensor type and will not appear as running sensor. It is a sensor that uses the meta-scan facility of the PRTG probe to find or match OIDs from an MIB and eases the creation of custom sensors, because you do not have to enter the OIDs manually.

To monitor SNMP capable devices and add sensors using the SNMP Library sensor, download the manufacturer's MIB files for the target device, convert the MIB file to the Paessler **oidlib** format, and import it into PRTG. To make setting up your monitoring as convenient as possible, PRTG comes with pre-compiled **oidlib** library files that already contain the OIDs of SNMP counters for the most common devices in a network.

 For more details, see the Knowledge Base: [How do SNMP, MIBs and OIDs work?](#)

Default OIDLIB Files Overview

The following files are included in PRTG and are ready to use with the SNMP Library sensor. These allow the extension of your SNMP monitoring to many devices. Please be aware that not all devices and/or parameters may be supported by the libraries.

- **APC UPS.oidlib**
Can be used to monitor uninterruptible power supplies (UPS) from APC American Power Conversion Corp.
- **APCSensorstationlib.oidlib**
Can be used to monitor alarm status, communication status, humidity, and temperature as shown by an APC sensor station.
- **Basic Linux Library (UCD-SNMP-MIB).oidlib**
Can be used to monitor basic system parameters on Linux systems, such as memory, disk and swap, CPU, etc.
- **cisco-interfaces.oidlib**
Can be used to monitor Cisco specific parameters, for example, the number of present network interfaces on a system, several states of an interface (admin, oper, speed, type, errors, discards, etc.), and more.

- **cisco-queue.oidlib**
Can be used to monitor queues on a Cisco interface, for example, queue depth and its maximum, discarded messages from the queue, the number of the queue within the queue set, etc.
- **Dell Storage Management.oidlib**
Can be used to monitor Dell storage devices. Possible parameters include disk arrays, battery and power supply, fan and temperature, virtual disk, etc.
- **Dell Systems Management Instrumentation.oidlib**
Can be used to monitor the hardware of Dell systems. Possible parameters include ACPower and battery, alerts, base board, Bios, BMC, chassis, COO, cooling, event log, firmware, IDE, keyboard, memory, port, network, processor, SCSI, system, temperature, USB, UUID, etc.
- **HP LaserJet Status.oidlib**
Can be used to monitor toner, paper, and jam status of an HP LaserJet printer.
- **Linux SNMP (AX BGP DisMan EtherLike Host).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Framework Proxy Not i v2).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (IP Net SNMP Not i OSPF RMON SMUX).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Linux SNMP (Source TCP UCD UDP).oidlib**
Can be used to monitor different aspects of Linux systems.
 This file may detect a very large number of interfaces. It may take a few seconds until the selection table is shown.
- **Paessler Common OID Library.oidlib**
Can be used to monitor many common hardware devices. It is used for several sensors and is encrypted.
- **SNMP Informant std.oidlib**
Can be used to monitor logical disks, processor, memory, and network interface on Windows systems.

More

Knowledge Base: How do SNMP, MIBs and OIDs work?

- <https://kb.paessler.com/en/topic/653>

Knowledge Base: My SNMP sensors don't work. What can I do?

Part 11: Sensor Technologies | 1 Monitoring via SNMP
1 Choosing the Right SNMP Sensor

- <https://kb.paessler.com/en/topic/46863>

Knowledge Base: How can I import my MIB files into PRTG?

- <https://kb.paessler.com/en/topic/733>

Knowledge Base: Can't find a sensor for my device in PRTG but I believe it supports SNMP. How to proceed?

- <https://kb.paessler.com/en/topic/65638>

11.2 Monitoring via WMI

You can monitor Windows systems via [Windows Management Instrumentation \(WMI\)](#)^[3507] and [Windows Performance Counters](#)^[3508]. WMI is the Microsoft base technology for monitoring and managing Windows-based systems. PRTG uses this technology to access data of various Windows configuration parameters and status values. However, sensors using the WMI protocol generally have a high impact on system performance. In addition to strict WMI sensors, there are sensors that can use Performance Counters to monitor Windows systems.

To monitor via WMI and Performance Counters, it is usually sufficient to provide **Credentials for Windows Systems** in PRTG. However, monitoring via WMI is not always trivial and often causes issues.



See this article in our Knowledge Base if you run into issues: [My WMI sensors don't work. What can I do?](#)

It is also possible to use Simple Network Management Protocol (SNMP) for Windows devices. The same information is often available using any of these protocols. From a performance perspective, the preference would be SNMP, and then WMI or Performance Counters.

How WMI Works

WMI allows accessing data of many Windows configuration parameters, as well as current system status values. Access can be local or remote via a network connection. WMI is based on **COM** and **DCOM** and is integrated in Windows versions as of Windows Server 2000. PRTG officially supports WMI for Windows 7 or later.



WoW64 (Windows 32-bit on Windows 64-bit) must be installed on target systems that run Windows Server 2016. This allows 32-bit applications to be run on 64-bit systems. This is necessary because the probe service only runs with 32-bit support. Without it, WMI sensors will not work.

To monitor remote machines, PRTG WMI sensors need Active Directory account credentials to have access to the WMI interface. You can enter these credentials in PRTG for the parent device or group, or in the [Root](#)^[334] group. The sensor will then inherit these settings.



Sensors using the Windows Management Instrumentation (WMI) protocol generally have a high impact on the system performance! Try to stay below 200 WMI sensors per [probe](#)^[125]. Above this number, please consider using multiple [Remote Probes](#)^[370] for load balancing.



For an overview and details about all WMI sensors, see the [List of Available Sensor Types](#)^[433] section.

Monitoring Windows Systems: Performance Counters

Besides sensor types that can monitor Windows systems only via WMI, PRTG provides sensor types that can use a **hybrid** approach. If you choose the hybrid approach, these sensors will first try to query data via Windows **Performance Counters** using **Remote Registry Service**. These Windows sensors use WMI as a fallback if Performance Counters are not available or cannot be read out. When running in fallback mode, PRTG re-tries to connect to Performance Counters after 24 hours. You can change the **Preferred Data Source** in the **Windows Compatibility Options** in the [Device Settings](#)^[402].

i You can identify these hybrid sensors by looking at their categories, for example, in the [Add Sensor](#)^[325] [dialog](#)^[325]. **Search directly** for "windows" and select "Performance Counters" as **Technology Used**. Among them are various sensors with "Windows" in the name, as well as some Hyper-V sensors.

Limitations of WMI on Windows Server 2008 (R1)

You should be aware that performance of WMI-based monitoring is drastically limited when the monitoring station or the monitored client runs on Windows Server 2008 (R1). When it comes to network monitoring via WMI, Windows Server 2008 R2 is many times faster than Windows Server 2008 (R1).

- i** These are not limitations of PRTG, but arise from the WMI functionality built into the Windows operating systems mentioned.
- i** These limitations also apply to Windows Vista, which is no longer officially supported. You can still monitor machines running Windows Vista, but PRTG core server and probes are no longer supported on this operating system.

The results of our tests are:

- On Windows Server 2008 R2 or Windows 7 (and on later Windows versions) you can run most WMI sensors if you provide optimal conditions, such as running the core and the target systems exclusively under Windows Server 2008 R2 and being located within the same LAN segment. Actual performance can be significantly less depending on network topology and WMI health of the target systems—we have seen configurations that could not go beyond 500 sensors (and even less).
- On Windows 2008 (R1) you can run about 300 WMI sensors with one minute interval.
- The more Windows 2008/Windows 7 client systems you have in your network, the more WMI monitoring performance will be affected.
- System performance (CPU, memory, etc.) of virtualization does not strongly affect WMI monitoring performance.

If you want to use WMI for network monitoring of more than 20 or 30 systems, please consider the following rules:

- Do not use Windows 2008 (R1) as monitoring stations for WMI-based network monitoring.
- Use Windows Server 2008 R2 (or later Windows versions) for WMI-based network monitoring instead.

- Consider setting up remote probes for the WMI monitoring. You still get far better WMI monitoring performance with a remote probe on a virtual machine running Windows Server 2008 R2 than on any bare metal system running Windows 2008.
- Consider switching to SNMP-based monitoring for large networks. Using SNMP you can easily monitor 10 times as many nodes as with WMI on the same hardware.

More

Knowledge Base: General introduction to WMI and PRTG

- <https://kb.paessler.com/en/topic/1043>

Video Tutorial: Bandwidth Monitoring with SNMP and WMI

- <https://www.paessler.com/support/videos/prtg-basics/bandwidth-monitoring-basic>

Knowledge Base: Which WQL queries are used by PRTG's WMI sensors?

- <https://kb.paessler.com/en/topic/8783>

Tool: Paessler WMI Tester. A useful freeware tool to test WMI connections. Tests the accessibility of WMI (Windows Management Instrumentation) counters in a quick and easy manner.

- <https://www.paessler.com/tools/wmitester>

11.3 Monitoring via SSH

Monitoring via Secure Shell (SSH) enables you to gather performance and system data from many Linux and Unix distributions, as well as from certain Mac OS X systems. If your system is supported, this monitoring technology will work without any additional software on the target systems.

How Monitoring via SSH Works

To monitor remote machines via SSH, PRTG needs the credentials (preferably root access) of the devices. If you use SSH sensors with PRTG, you can enter the necessary credentials in PRTG for the parent device or group, or in the [Root](#) group, in the [Credentials for Linux/Solaris/Mac OS \(SSH/WBEM\) Systems](#) section on the [Settings](#) tab. The sensors then inherit these settings by default.

With each scanning interval, PRTG logs in to your devices and queries data by executing specific commands.

 For an overview and details about all SSH sensors, see the [List of Available Sensor Types](#).

Limitations When Using SSH Monitoring

Due to the plurality of Linux/Unix derivatives, SSH sensors cannot support all distributions on the market. Also, only certain Mac OS systems are supported.

 For a list of successfully tested distributions, see this Knowledge Base article: [Which Linux or Mac OS distributions are supported by the Linux/Unix sensors \(SSH, SNMP\)?](#)

Authentication via SSH Private Key

PRTG supports authentication via password or via private key.

When you use a private key, please ensure the following:

- Provide the key in [OpenSSH RSA](#) format.
- The key may **not** be encrypted! PRTG does **not** support password-protected keys.
- The key must be provided as an [RSA](#) key, you cannot use [DSA](#) keys with PRTG!

When you provide an unencrypted RSA private key in OpenSSH RSA format, please copy the entire key, including the

```
-----BEGIN RSA PRIVATE KEY-----
```

and

```
-----END RSA PRIVATE KEY-----
```

lines, into the designated text field in PRTG and **Save** your settings. Once you have pasted in and saved the private key, PRTG shows it as

```
*****
```

Please make sure a corresponding public key exists on the target device.



For a detailed description on how to convert and use an existing SSH key, see this Knowledge Base article: [How can I use private keys for my SSH sensors with PRTG?](#)

More

Knowledge Base: Which Linux or Mac OS distributions are supported by the Linux/Unix sensors (SSH, SNMP)?

- <https://kb.paessler.com/en/topic/6733>

Knowledge Base: How can I use private keys for my SSH sensors with PRTG?

- <https://kb.paessler.com/en/topic/32883>

Knowledge Base: How do I enable SSH on my Mac OS X system?

- <https://kb.paessler.com/en/topic/33113>

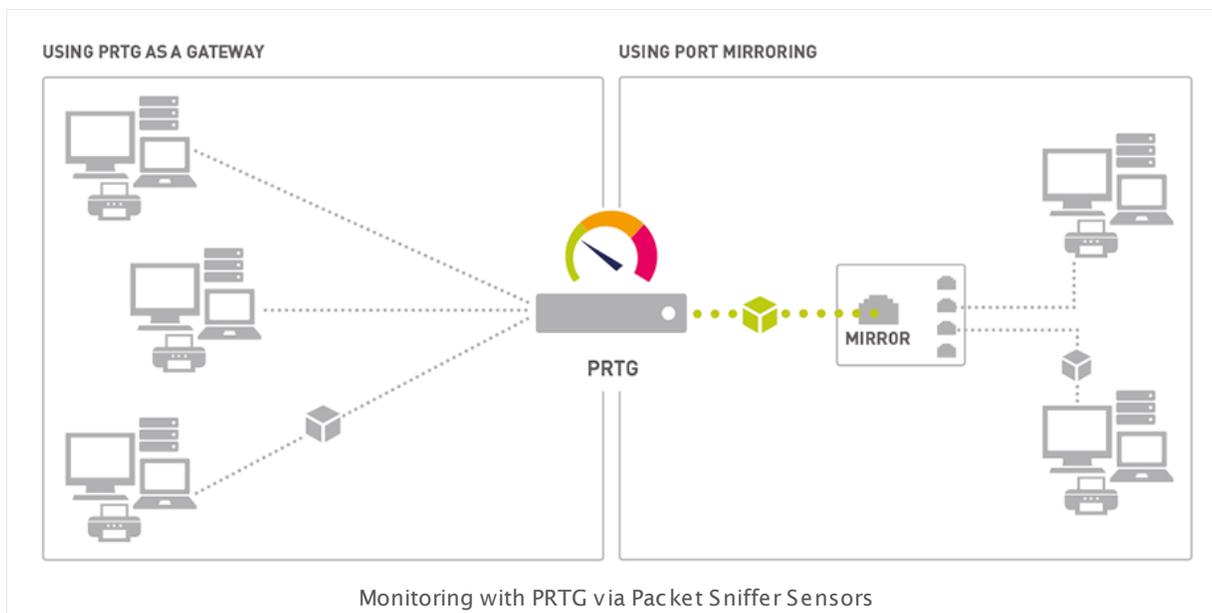
11.4 Monitoring Bandwidth via Packet Sniffing

Packet sniffing comes into consideration if your network devices do not support SNMP or xFlow to measure bandwidth usage and if you need to differentiate the bandwidth usage by network protocol and/or IP addresses.

❶ Packet Sniffer sensors support [Toplists](#)³¹⁸⁶ (Top Talkers, Top Connections, etc.).

How Packet Sniffing Works

If you need to know what applications or IP addresses cause the traffic in your network, you can use a packet sniffer. A packet sniffer looks at every single data package that travels through your network for accounting purposes.



PRTG can analyze the packets passing the network card of a PC or you can connect it to the **monitoring port** of a switch. To calculate bandwidth usage, PRTG inspects all network data packets either passing the PC's network card (shown on the left side in the schema above) or the data packages that a monitoring port of a switch (right side) sends with its built-in packet sniffer. Using remote probes, you can set up packet sniffers anywhere in your network (see [Add Remote Probe](#)³⁷⁰⁷ section).

[Comparing](#)³⁵¹⁷ the four bandwidth monitoring technologies that PRTG provides (SNMP, WMI, xFlow, and packet sniffer) this one creates the most CPU and network load, so you should only use it in small to medium-sized networks, on dedicated computers for larger networks or for individual computers.

Reasons to Choose Packet Sniffing

It is important to understand that the packet sniffer can only access and inspect data packages that actually flow through the network interface(s) of the machine running the PRTG probe software. This is fine if you only want to monitor the traffic of this machine (for example, your web server). In switched networks, only the traffic for a specific machine is sent to each machine's network card, so PRTG can usually not discern the traffic of the other machines in the network.

If you also want to monitor the traffic of other devices in your network, you must use a switch that offers a **monitoring port** or **port mirroring** configuration (Cisco calls it **SPAN**). In this case, the switch sends a copy to the monitoring port of all data packages traveling through the switch. As soon as you connect one of the PRTG probe system's network cards to the switch's monitoring port, PRTG is able to analyze the complete traffic that passes through the switch.

Another option is to set up the PC running PRTG as the gateway for all other computers in the network.

Set Up Packet Sniffer Sensors

Find details on how to set up the different flow sensors in the following sections:

- [Packet Sniffer Sensor](#) 1484
- [Packet Sniffer \(Custom\) Sensor](#) 1497

Header Based Packet Sniffing

For packet sniffing, PRTG looks at the IP addresses and ports of source and destination to assess the protocol. This is a very fast method and saves system resources.

i Sometimes, this method is not fully accurate. For example, it is not possible to identify HTTP traffic on ports other than **80**, **8080**, and **443** as HTTP. HTTP traffic on non-standard ports would not be accounted as such.

More

Video Tutorial: Bandwidth Monitoring With Flows and Packet Sniffing

- <https://www.paessler.com/support/videos/prtg-advanced/bandwidth-monitoring-advanced>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

11.5 Monitoring Bandwidth via Flows

Using flow protocols, you can monitor the bandwidth usage of all packets going through a device. In PRTG, you can view [Toplists](#) for all xFlow (NetFlow, IPFIX, sFlow, jFlow) sensors.

Flows are a type of monitoring data pushed from network devices to PRTG. You can use it to monitor where data is traveling to and from, and how much. This way it determines which machine, protocol, and user is consuming bandwidth. PRTG currently supports the following flow types:

- NetFlow v5/v9 and IPFIX: Originally introduced by Cisco and supported by several vendors
- jFlow: Traffic sampling technology introduced by Juniper networks
- sFlow: Short for sampled flow, introduced by HP. sFlow uses statistical sampling of the traffic at defined intervals to achieve scalability for high volume interfaces.

You can also use [packet sniffing](#) for bandwidth monitoring if your hardware does not support any of these flow versions.

How xFlow Monitoring works

You can measure bandwidth usage **by IP address** or **by application** in a network, using one of the xFlow (including IPFIX) protocols. They are the best choice especially for networks with high traffic (connections with hundreds of megabits or gigabits).

For xFlow monitoring, the router gathers bandwidth usage data (**flows**), aggregates them, and sends information about these flows to PRTG using UDP packets. When you use sampling (mandatory for sFlow), only information about every n-th packet is sent to PRTG, which reduces CPU load a lot. Because the switch already performs a pre-aggregation of traffic data, the flow of data to PRTG is much smaller than the monitored traffic. This makes xFlow the ideal option for high traffic networks that need to differentiate the bandwidth usage by network protocol and/or IP addresses.

NetFlow and IPFIX Monitoring

The NetFlow (and IPFIX) protocol is mainly used by Cisco devices. Once configured, the router sends for each data flow a NetFlow or IPFIX packet to the monitoring system running on a PRTG probe. You can filter and evaluate the data in PRTG. There are different NetFlow and IPFIX sensors available: The basic ones offer predefined channel definitions, the custom variants enable you to define your own channels.

The advantage of using NetFlow or IPFIX:

- Generates little CPU load on the router itself (according to Cisco, 10,000 active flows create about 7% additional CPU load; 45,000 active flows account for about 20% additional CPU load).
- Generates less CPU load on the PRTG core system compared to packet sniffer sensors.

i You must enable NetFlow or IPFIX export on the device you want to monitor. The device must send a flow data stream to the IP address of the PRTG probe system on which you set up the NetFlow or IPFIX sensor.

i You can monitor Juniper **jFlow** with the corresponding sensors as well. Basically they are adjusted NetFlow v5 sensors.

i **NetFlow Lite** monitoring is possible using the **Sampling Mode** of the [NetFlow V9 sensor](#)¹⁴³⁰ or of the [NetFlow V9 \(Custom\) sensor](#)¹⁴⁴⁴. You can turn on the sampling mode and define a suitable **Sampling Rate** in the [sensor settings](#)¹⁴³³. Please note that NetFlow Lite monitoring might not work in every case even with active sampling mode.

sFlow Monitoring

sFlow works similar to NetFlow monitoring. The router sends data flow packets to the monitoring system running on a PRTG probe. The most obvious difference between the two flow protocols: With sFlow, not all of the traffic is analyzed, but only every n-th packet. It is like having a river of traffic and you take a cup of water out of it ever so often and analyze it.

The advantage is clear: There is less data to analyze, there is less CPU load needed, and less monitoring traffic is generated. Nevertheless, you can get a good insight into your network bandwidth usage.

i PRTG supports sFlow version 5.

Set Up Flow Sensors

Find details on how to set up the different flow sensors in the following sections:

- [NetFlow V5 Sensor](#)¹⁴⁰³
- [NetFlow V5 \(Custom\) Sensor](#)¹⁴¹⁷
- [NetFlow V9 Sensor](#)¹⁴³⁰
- [NetFlow V9 \(Custom\) Sensor](#)¹⁴⁴⁴
- [IPFIX Sensor](#)¹¹⁸⁶
- [IPFIX \(Custom\) Sensor](#)¹²⁰⁰
- [sFlow Sensor](#)¹⁷⁴⁰
- [sFlow \(Custom\) Sensor](#)¹⁷⁵⁴
- [jFlow V5 Sensor](#)¹²²³
- [jFlow V5 \(Custom\) Sensor](#)¹²³⁷

Limitations

On a powerful 2008 PC (Dual Core, 2.5 Ghz), you can process about 100,000 flows per second for one xFlow stream. Using sampling, the number of actual flows can be much higher. When using complex filters, the value can be much lower. For example, with a router sending about 2,000 flows/second (which corresponds to mixed traffic at gigabit/second level without sampling) you can expect to configure up to 50 NetFlow sensors operating properly.

PRTG internally monitors its own NetFlow processing. You can see decreased values in the **Health** channels of the **Core Health**⁶⁵² and **Probe Health**¹⁵⁹⁰ sensors as soon as NetFlow packets are not processed due to an overload (you find these sensors on the local probe device).

If you experience an overload, please consider using sampling or setting up multiple probes and distribute the NetFlow streams to them. We recommend that you do not add more than 50 NetFlow sensors per PRTG probe.

This sensor type cannot be used in cluster mode. You can set it up on a local probe or remote probe only, not on a cluster probe.

 IPv6 flows are supported by NetFlow V9 and IPFIX sensors, other flow sensor types only support IPv4.

More

Video Tutorial: Bandwidth Monitoring With Flows and Packet Sniffing

- <https://www.paessler.com/support/videos/prtg-advanced/bandwidth-monitoring-advanced>

Knowledge Base: Can I add custom channels to standard Packet Sniffer and NetFlow sensors?

- <https://kb.paessler.com/en/topic/2143>

Knowledge Base: What filter rules can be used for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors?

- <https://kb.paessler.com/en/topic/483>

Knowledge Base: How do the channel definitions for custom Packet Sniffing or xFlow (NetFlow/sFlow) sensors work?

- <https://kb.paessler.com/en/topic/473>

Knowledge Base: Does my Cisco device (Router/Switch) support NetFlow Export?

- <https://kb.paessler.com/en/topic/5333>

Knowledge Base: Do you have any configuration tips for Cisco routers and PRTG?

- <https://kb.paessler.com/en/topic/563>

Knowledge Base: How to monitor Cisco ASA Firewalls using NetFlow 9 and PRTG?

- <https://kb.paessler.com/en/topic/1423>

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

Knowledge Base: What is the Active Flow Timeout in Flow sensors?

- <https://kb.paessler.com/en/topic/66485>

Tools: NetFlow Generator and NetFlow Tester

- <https://www.paessler.com/tools/>

11.6 Bandwidth Monitoring Comparison

The following table shows the differences between the four bandwidth monitoring methods available in PRTG:

	WMI <small>3507</small>	SNMP <small>3489</small>	Packet Sniffer <small>3512</small>	xFlow (IPFIX, NetFlow, sFlow, jFlow) <small>3514</small>
Setup	Medium	Easy	Easy to complex (depending on filter rules used)	Can be complex (for example, the switch must be configured)
Traffic can be filtered	No	No	Yes	Yes
Differentiate bandwidth usage by protocol or IPs	No	No	Yes	Yes
PRTG can show Toplists (Top Talker, Top Connections, Top Protocols, custom)	No	No	Yes	Yes
Filter bandwidth usage by IP	No	No	Yes	Yes
Filter bandwidth usage by MAC address	No	No	Yes	No
Filter bandwidth usage by physical network port	Yes	Yes	No	No

	WMI <small>3507</small>	SNMP <small>3489</small>	Packet Sniffer <small>3512</small>	xFlow (IPFIX, NetFlow, sFlow, jFlow) <small>3514</small>
Monitor network parameters other than bandwidth usage	Yes	Yes	No	No
CPU load on the machine running PRTG	Low	Low	Higher, depends on the amount of traffic	Higher, depends on the amount of traffic
Excess bandwidth usage of monitoring	Small	Small	None (except when monitoring switch ports are used)	Depends on the traffic

More

Knowledge Base: Should I use SNMP, xFlow (IPFIX/NetFlow/sFlow) or Packet Sniffing for my monitoring?

- <https://kb.paessler.com/en/topic/923>

Knowledge Base: How do I discern excessive bandwidth usage with PRTG?

- <https://kb.paessler.com/en/topic/2923>

11.7 Monitoring Quality of Service and VoIP

PRTG can monitor the Quality of Service (QoS) in a network with dedicated QoS sensors, as well as Cisco IP Service Level Agreement (SLA) and Cisco Class Based Quality of Service (CBQoS). Slight variations of network parameters like jitter, packet loss, or packet delay variation (PDV) usually have only little effect on TCP-based services (for example, HTTP and SMTP). But for UDP-based services like Voice over IP (VoIP) and video streaming, a steady stream of data packets is crucial. The sound quality of a VoIP call drops dramatically when UDP packets are not received in a timely fashion, or if packets are lost or out-of-order.

As a rule of thumb for good quality of service (from a VoIP perspective), you want low measurements for jitter (less than 20 to 50 ms) and PDV (less than 100 ms), and preferably **zero** measurements for packet loss, duplicated packets, or packets in wrong order.

For Quality of Service measurements, four sensor types are available:

- [QoS \(Quality of Service\) Sensor](#)^[1608]
Monitors VoIP-relevant network parameters by testing the network connection quality between two probes.
- [QoS \(Quality of Service\) Round Trip Sensor](#)^[1617]
Monitors VoIP-relevant network parameters by testing the network connection quality between a probe and a target device at the endpoint of the connection. Traffic is measured bidirectionally.
- [Cisco IP SLA Sensor](#)^[589]
Monitors VoIP-relevant network parameters through IP SLA results from Cisco devices (via SNMP).
- [SNMP Cisco CBQoS Sensor](#)^[1887]
Monitors VoIP-relevant network parameters by using Cisco's CBQoS (via SNMP).

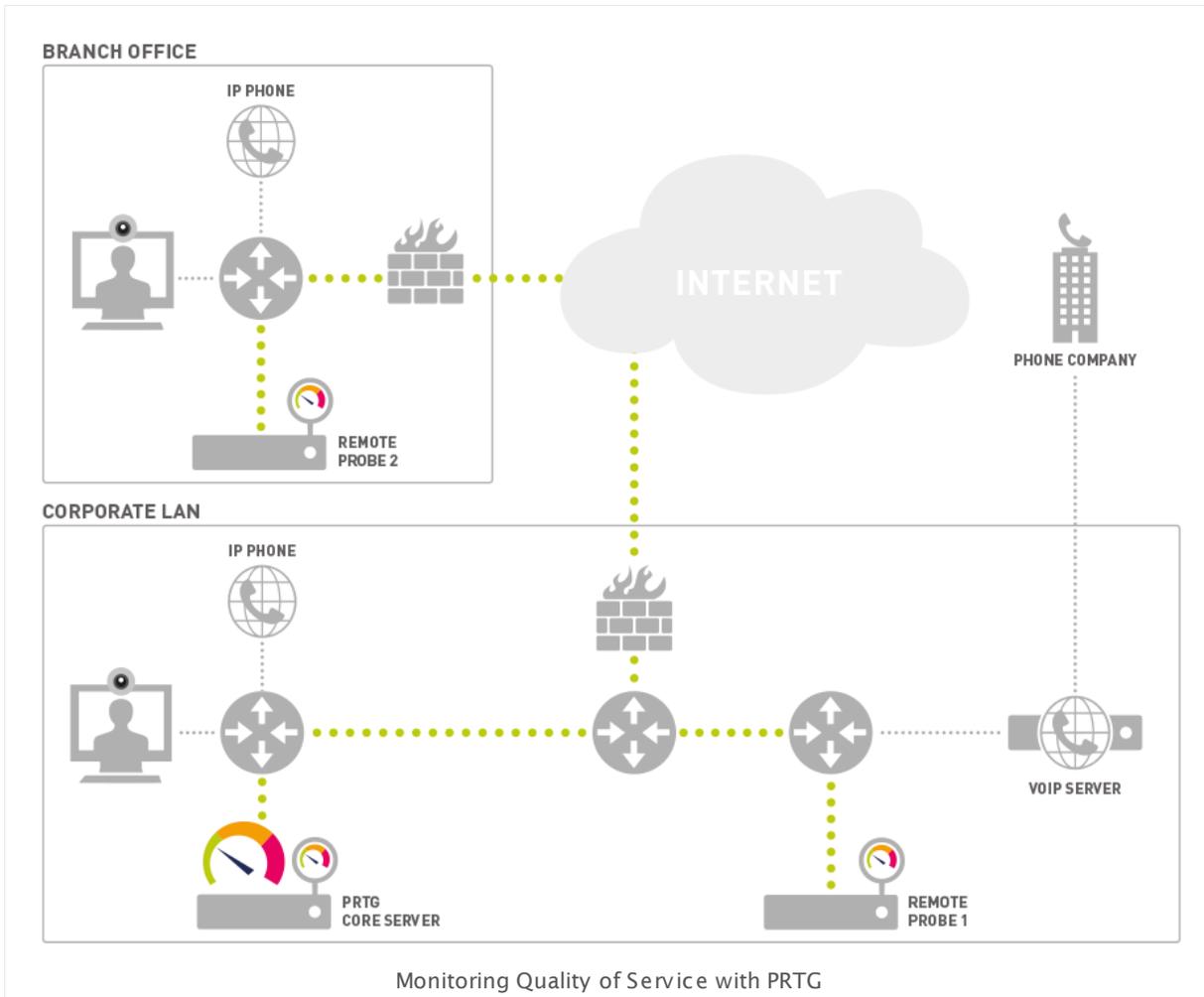
QoS (Quality of Service) Sensors

The QoS Sensors monitor the quality of a network connection by measuring the following parameters:

- Jitter in ms according to RFC 3550
- Packet delay variation (PDV) in ms according to RFC 3393
- Lost packets in %
- Out-of-order packets in %
- Duplicated packets in %

The QoS sensors measure quality of service by sending UDP packets between two probes. This means that you can test any network connection in your network by simply placing a [remote probe](#)^[3707] on (or near) each 'end' of the connection and measuring the connection quality between them. This is the perfect tool to find network issues that can affect VoIP sound quality or video streaming 'hiccups'.

 You can use the QoS Round Trip sensor also without installing a remote probe at the connection endpoint. See this Knowledge Base article for details about the PRTG QoS Reflector: [How can I monitor QoS roundtrips without using remote probes?](#)



The measurements for QoS monitoring are taken between two probes. So the first step is to place two PCs running a remote probe on (or near) both ends of the connection that you want to monitor. As an alternative, the local probe on the PC running the PRTG core can also be used as one end, or you can use the PRTG QoS Reflector (see the [Knowledge Base](#)) to bounce the packets when monitoring QoS roundtrips. If any firewalls, packet filters, or Network Address Translation (NAT) systems are en route, you must configure them as necessary so that the UDP packets can reach the target probe.

In PRTG, create a new QoS sensor on a **Probe Device**, or, if you use the roundtrip sensor, on any device. With the settings for number and for size of the packets, you can configure the test data stream. 1,000 packets of 172 bytes each is a good start, but if your applications use larger packets, you may want to enter other values here. Try to configure the test streams with parameters similar to that of the UDP services you are using across this connection.

 Find details about settings in the manual sections [QoS \(Quality of Service\) One Way Sensor](#)^[1608] and [QoS \(Quality of Service\) Round Trip Sensor](#)^[1617].

Cisco IP SLA Sensor

Wikipedia describes IP SLA as **a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services. IP SLA uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance.** IP SLA is mostly used to monitor the sound quality of VoIP traffic.

If you have not done so already, add a device in PRTG for the Cisco device that you want to monitor. Then create a new **Cisco IP SLA** sensor on this device.

 Find details about settings in the [Cisco IP SLA Sensor](#)^[589] section.

This feature is only available in the more expensive Cisco devices. If you do not have IP SLA capable routers and switches, you can still get similar information with PRTG QoS sensors (see [above](#)^[3516]) that do not require any special hardware—just two PCs running Windows. If you own hardware that supports IP SLA, then PRTG brings you probably the least-cost monitoring solution for IP SLA. Most vendors charge extra for IP SLA support (a thousand bucks and more). Following Paessler's long term policy, we simply include this as one of our sensor types. With PRTG you can even use the PRTG on premises Freeware Edition to monitor IP SLA!

PRTG monitors the following parameters: Calculated Planning Impairment Factor (ICPIF), Mean Opinion Score (MOS), Average Jitter, Packets Lost, Packets Out Of Sequence, Packets Late, Average Round Trip Time (RTT), DNS RTT, TCP RTT, Transaction RTT.

Especially two of these parameters are interesting for VoIP: **Mean Opinion Score (MOS)** and **Calculated Planning Impairment Factor (ICPIF)**.

SNMP Cisco CBQoS Sensor

Cisco Class Based Quality of Service (CBQoS) provides information about QoS of Cisco network devices that support the **Modular QoS command line interface (MQC)**. With Classed Based QoS, you can obtain monitoring data that includes summary counts and rates by traffic class before and after the enforcement of QoS policies, according to Cisco's CBQoS Management Information Base (MIB) definition.

PRTG determines CBQoS data via Simple Network Management Protocol (SNMP). The corresponding sensor type is available out-of-the-box in PRTG version 13.x.5 or later. CBQoS is available in Cisco IOS by default as of version 12.4(4)T.

To monitor CBQoS, add a device to PRTG for the Cisco device that you want to monitor. Then create a new SNMP Cisco CBQoS sensor on this device.

 See section [SNMP Cisco CBQoS Sensor](#)^[1687] for more details.

This sensor type supports the following CBQoS classes:

- **Class Map:** statistical data about class maps, such as pre- and post-policy packets and sizes, drop packets and size, as well as no-buffer drop packets

- **Match Statement**: statistical data about match statement specific information, such as pre-policy packets and size
- **Queueing**: statistical data about queuing actions, such as current and maximum queue depth, drop packets, and drop size

You can select the desired CBQoS entries that you want to monitor while creating the sensor in PRTG. The available entries are given with their particular connections, their descriptions, and class types.

Voice over IP

For Mean Opinion Score (MOS) measurements, Cisco conducted a panel test where a wide range of listeners judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The Cisco device calculates the corresponding value for the current network connection based on the network parameter measurements like jitter and packet loss.

 The Cisco IP SLA sensor reads out the MOS directly from the Cisco device. For the QoS and the QoS Round Trip sensor, PRTG calculates the MOS by itself. For details, see this Knowledge Base article: [How does PRTG calculate the MOS score for QoS sensors?](#)

The values and their meanings are:

MOS	Quality	Expected Quality Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The second interesting parameter ICPIF is the sum of measured impairment factors minus a user-defined access Advantage Factor that is intended to represent the user's expectations, based on how the call was placed (for example, a mobile call versus a land-line call) (quoted from Cisco's website).

Upper Limit for ICPIF	VoIP Call Communication Quality
5	Very good

Upper Limit for ICPIF	VoIP Call Communication Quality
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

More

Knowledge Base: Where can I find more information about Cisco IP SLAs, VoIP, and QoS?

- <https://kb.paessler.com/en/topic/11093>

Knowledge Base: How does PRTG calculate the MOS score for QoS sensors?

- <https://kb.paessler.com/en/topic/59491>

Knowledge Base: How can I monitor QoS roundtrips without using remote probes?

- <https://kb.paessler.com/en/topic/61176>

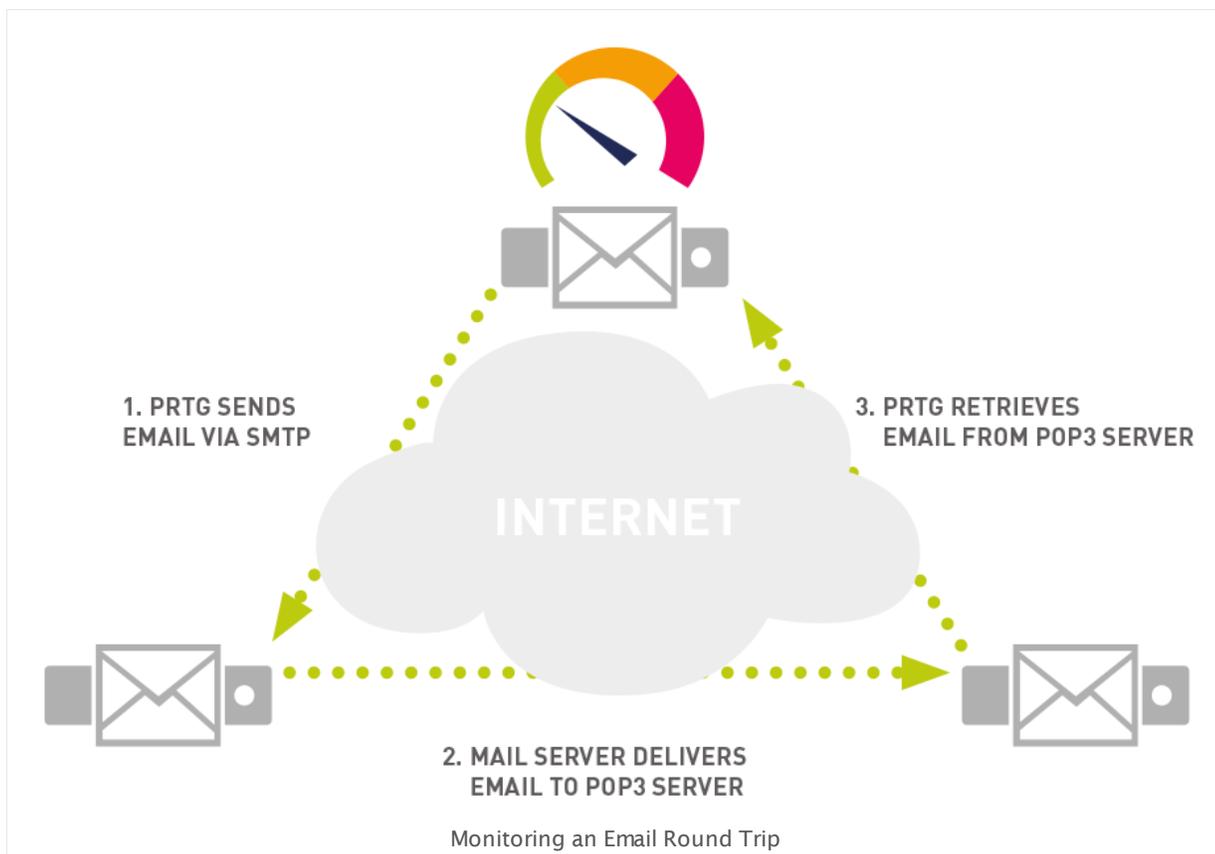
11.8 Monitoring Email Round Trip

Email Round Trip sensors ensure the end-to-end delivery of emails and make it possible to monitor availability and performance of a complete email delivery process. There are two sensor types for this task:

- [SMTP&POP3 Round Trip Sensor](#) 1817
- [SMTP&IMAP Round Trip Sensor](#) 1805

Both initially deliver an email to a mail server using SMTP. Afterwards the receiving mailbox is scanned using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP) until the email arrives. The test email contains a unique code in the topic that is used to identify the email, such as **PRTG Roundtrip Mail: {6D136420-5A3E-46CF-871A-1DAF0C4F3D5D}**

When PRTG successfully receives an email in this email round trip cycle, it marks the respective message for deletion on the mail server. Usually, a mail server will then delete this email. For best performance, we recommend using a dedicated email accounts for email round trip sensors.



In the scenario shown above, there are three steps in the round trip:

- **Step 1**
PRTG delivers an email via the SMTP protocol to a mail server (just like an email client).

- **Step 2**
The SMTP server delivers the email to a POP3/IMAP server (which can be located at a remote site, in your local LAN, or on the same server as well).
- **Step 3**
Every few seconds PRTG connects to the POP3/IMAP server until the test email arrives.

Recommended Configuration

Here is a simple concept to check the delivery of email out of and into your organization:

1. Create a dedicated email account for this test in your mail system.
2. Set up an external email account (hosted mail server, free mail service, etc.) and configure it to send all emails back to this dedicated email account in your organization (that you created in [Step 1](#)).
3. Set up a PRTG round trip sensor to send an email to the external email account (that you created in [Step 2](#)) using your network's mail server and then check for the email account on your mail system (that you created in [Step 1](#)) for the arrival of the email.

With this technique, you are testing multiple aspects of your email server setup. As long as the sensor shows a green light, this means:

- Your email server accepts emails via SMTP.
- Emails are being sent to the outside world (internet connection works, MX lookups work, etc.).
- Emails from an external mail server can be delivered into your mail system (this includes aspects like the fact that the MX records for your domain are correct, your mail server can be reached from the outside world, your email filtering is working, etc.).
- Emails can be retrieved using POP3 (or IMAP).

Please use dedicated email accounts with this sensor type. If you use more sensors of this type, please make sure that each sensor uses its own email accounts.

Conclusion

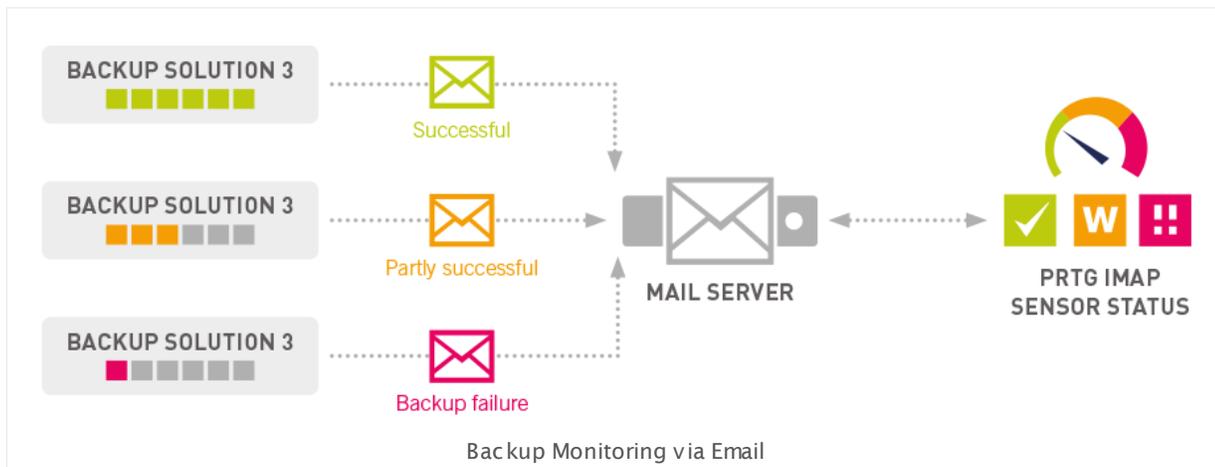
These two sensor types are a great tool to ensure the delivery of email from and to your mail servers. Compared to the standard SMTP, POP3, and IMAP sensors, which only check the availability of these services, the two roundtrip sensor types actually monitor the complete transaction from accepting the email on the first email server to the delivery of the email on the final POP3/IMAP server.

11.9 Monitoring Backups

Monitoring your backup software enables you to be sure that your recent backups succeeded. With PRTG you can check the email notifications of various backup jobs. You only need two things for backup monitoring:

1. Configure your backup software to send emails to a dedicated email account.
2. Configure the PRTG [IMAP Sensor](#)¹¹⁶² for backup monitoring.

PRTG will analyze the backup emails for you and set the status of the IMAP sensor accordingly. This way you will see the states of all your backup jobs at a glance.



Setting up Backup Monitoring

 Refer to our Knowledge Base for a step-by-step tutorial to monitor your backup jobs: [Monitoring Backup Solutions via Email](#)

More

Knowledge Base: Monitoring Backup Solutions via Email

- <https://kb.paessler.com/en/topic/47023>

Knowledge Base: Can I analyze multipart emails using the PRTG IMAP sensor?

- <https://kb.paessler.com/en/topic/63532>

11.10 Monitoring Virtual Environments

A highly flexible IT infrastructure is a common need nowadays and virtualization has become an important pillar of IT all over the world. Applications in your network might be distributed over many different servers, networks, and locations. They might also be in the cloud, and your computations can take place in datacenters spread over the whole world. So, if your network connection or any other corresponding hardware fails, hundreds of applications might be unavailable—an impact on your daily business processes that should be avoided at any costs.

Because of this, monitoring the physical infrastructure of your datacenter is still a must in times of virtual environments. With the layer of virtualization in addition to your physical equipment, your logical infrastructure also needs a close treatment. PRTG assists you in dealing with these advanced requirements and enables you to proactively react to issues before they affect your whole system. With PRTG you can monitor all layers of your IT infrastructure in a comprehensible way so you will significantly reduce issues related to dynamic IT environments.

Monitoring All Layers of Your IT Infrastructure

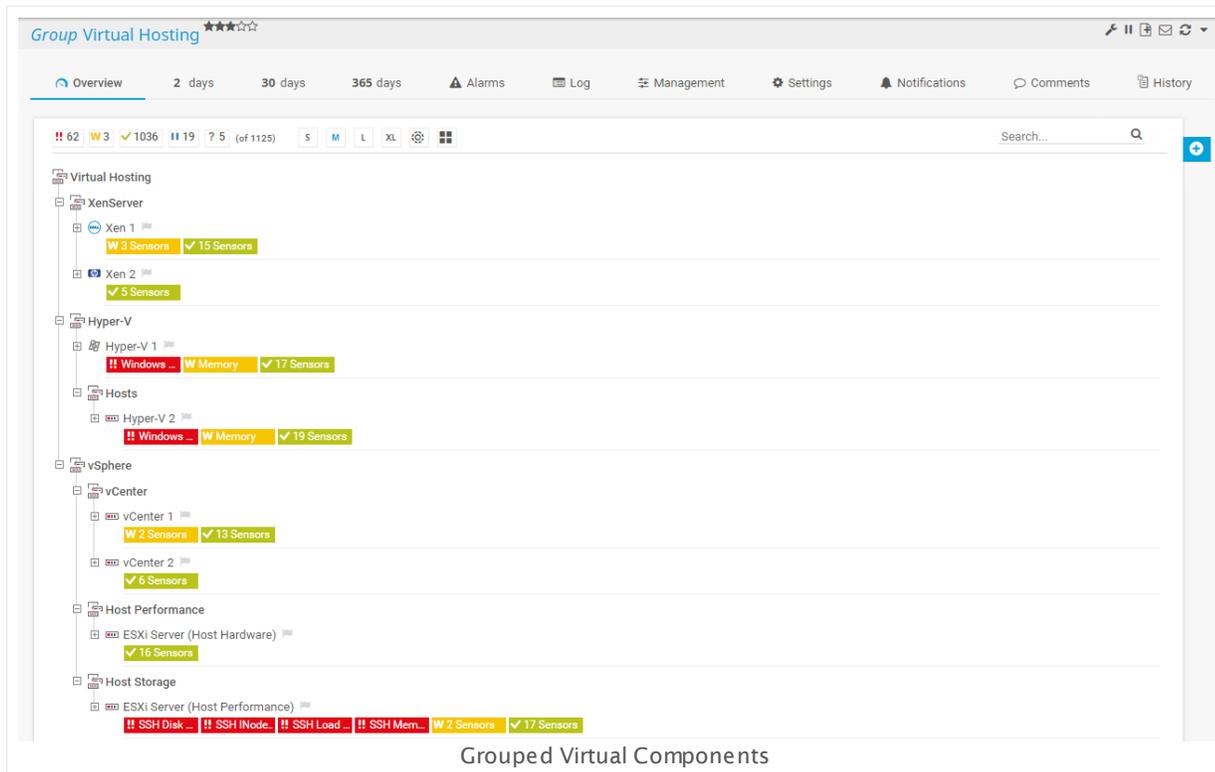
In general, you can assume that with the layer of virtualization, you have to monitor a total of four layers in your IT infrastructure:

- **Hardware (Server Racks):** Usually you will set up your monitoring in the common way and monitor most of the hardware components in your network with [PRTG's SNMP sensors](#)^[431]. You are able to gain monitoring data about many different device readings such as CPU load, memory, disk space with [this monitoring technology](#)^[3489], as well as information about network traffic and bandwidth usage of your routers and switches. It is absolutely mandatory for a working IT environment to monitor all hardware components in order to be alerted if something fails or hardware resources are running out. In addition, you can identify potential bottlenecks affecting your virtualized infrastructure. You can set up this monitoring in the usual way.
- **Host Server Hardware:** It is essential to explicitly monitor the host hardware of your virtualization solution. If you have issues with your virtual machines (VMs), the origin might be a host hardware failure. You should closely monitor your VM host servers to get alerted if the status is other than "normal". Besides the out-of-the-box hardware sensors, PRTG provides specific sensors for various virtualization host servers; the following monitoring data of your host servers will help you prevent issues in virtualized environments:
 - VMware: current reading and health status (via WBEM), a general status as shown in vSphere (via SOAP), and disk space of a VMware data store (via SOAP)
 - Hyper-V: host health critical values, deposited pages, network traffic, CPU usage of guests, hypervisor, and in total
 - Citrix XenServer: CPU, memory, and network usage, the number of running virtual machines on the host server, and load average

- **VMs from the "Outside":** The virtual machines run on their particular host servers. PRTG can show you the status of single virtual machines and several of their performance counters. It might be helpful to know which resources a single VM uses and needs, but monitoring single VMs is not advisable in every case because it has a noticeable influence on the overall performance. Often it will be sufficient to monitor only VMs that are critical for your network. If a VM reaches its capacity limits, PRTG can alert you and you can conduct the corresponding resolution steps like enhancing this VM's resources. Indicators for a healthy virtual machine that you can monitor with PRTG out of the box are:
 - VMware: CPU and memory usage, disk read and write speed, read and write latency, and network usage
 - Hyper-V: CPU usage, disk read and write speed
 - Citrix XenServer: CPU usage and free memory
- **VMs from the "Inside" (Operating Systems):** You can monitor the Windows operating system of a single VM with PRTG's standard [WMI sensors](#)^[433], for example. [With this technology](#)^[3507] you can access data of various Windows parameters. Other operating systems like Linux/macOS can make data available via [SSH](#)^[3510] and [SNMP](#)^[3489]. The status of the operating systems on your VMs can indicate potential issues of the same, just like the operating systems on your physical machines that are important for a reliably working IT infrastructure: You can monitor these with the same attention, depending on your application scenario, but be careful due to performance considerations. Especially many WMI sensors can result in load problems, so monitor only really important systems "from the inside". Furthermore, you do not need to monitor every item multiple times. For example, it might be sufficient to monitor free disk space only from the outside of the actual VM.

Monitoring the Virtual Infrastructure

To monitor your IT infrastructure, best practice is to set up the monitoring of the hardware layer of your datacenter first in PRTG, especially in order to find potential bottlenecks that might have an impact on your virtual servers. Then you can start monitoring your virtual environment itself. If you use several solutions for virtual hosting, it is also a good idea to group related host servers, their virtual machines, and the operating systems together. The screenshot below will give you an idea about how to organize this.



The screenshot above shows you the particular group "Virtual Hosting" of an entire PRTG setup. This is an example of how monitoring of virtual environments can look. The sample group contains several subgroups for the virtualization solutions Citrix "XenServer", Microsoft "Hyper-V", and VMware "vSphere". The vSphere group, for example, has three subgroups: we monitor the vCenter VMs and the vCenter Windows system, the performance of the host server, and the storage system of the host.

Devices for Physical Hosts

In PRTG, set up devices that represent the physical hosts of your virtual machines. For example, for your VMware hosts, add devices that represent the ESXi servers, for Hyper-V add devices that represent your Hyper-V host servers, for Citrix add devices that represent your Xen servers.

Then you can add suitable and expressive sensors to the host server devices. Running the PRTG [auto-discovery](#)^[282], many useful sensors will be created automatically. There are several pre-configured host hardware sensors available out of the box in PRTG:

- [VMware Host Hardware \(WBEM\) Sensor](#)^[2703]: monitors an ESXi server via Web-Based Enterprise Management (WBEM)
- [VMware Host Hardware Status \(SOAP\) Sensor](#)^[2713]: monitors a VMware host server via Simple Object Access Protocol (SOAP)
- [VMware Host Performance \(SOAP\) Sensor](#)^[2723]: monitors a VMware host server via Simple Object Access Protocol (SOAP)

- [Hyper-V Host Sensor](#)^[1121]: monitors via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device
- [Citrix XenServer Host Sensor](#)^[599]: monitors via Hypertext Transfer Protocol (HTTP)

These sensor types monitor hardware-specific counters to ensure that no hardware issues affect your actual virtual machines. Additional sensor types can monitor the host hardware via SNMP (for example, traffic and custom requests), data storage on ESXi servers via SOAP, as well as sensors for network adapters and storage devices that are connected to a Hyper-V host server.

Devices for Virtual Machines

To monitor your actual virtual machines, add them to your host servers in PRTG. For a better overview, you might want to add another device to PRTG that represents your host server and add sensors for your VM there. The according sensors for virtual machines will show you the performance of single VMs as well as their usage of resources. This will help you identify VMs with poor performance and react proactively before one or more VMs crash. As mentioned above, you can additionally monitor your particular VMs from the inside (which means the operating systems on your VMs) if necessary. See the sections below for details about particular virtualization solutions.

VMware Virtual Machine

The [VMware Virtual Machine \(SOAP\) Sensor](#)^[2733] monitors VMs on a VMware host server via Simple Object Access Protocol (SOAP). With the VMware system, the general idea is to add a **vCenter** server as a device to PRTG and use the vCenter as parent device where you add the sensors for your virtual machines. So, in the case of **vMotion** when your VMs change their host server, PRTG will be able to follow these movements and will never lose the monitored VMs.

For this sensor type, you need the **Microsoft .NET Framework** version 4.5 or later running on the probe machine. If you use many VMware sensors, we also recommend adjusting the settings on your VMware host server to accept more incoming connections.

The screenshot displays the PRTG Network Monitor interface for a vSphere group. The interface is organized into several sections:

- vCenter:** Contains sensors for PING (0 msec), Memory (42%), HTTP (40 msec), RDP (16 msec), and various network and disk metrics.
- Host Performance:** Contains sensors for Power Supply (230 Volt), Processor (63 °C), and System Board (3,360 RPM).
- Host Storage:** Contains sensors for SSH Disk, SSH INode, SSH Load, and SSH Mem.

The status bar at the bottom indicates the overall health of the group, showing 62 critical issues, 3 warnings, 1036 OK, and 19 unknown sensors.

This screenshot shows a sample vSphere group in PRTG. As recommended, the VMware virtual machines are added to the vCenter device. There is also a dedicated device for the vCenter Windows operating system with common WMI sensors for CPU, memory, disk, and network usage. The ESXi host servers are organized in their own groups regarding performance and storage. In this example, PRTG monitors the hosts with the standard SNMP hardware sensors as well as with the specific VMware ESXi host sensors.

Microsoft Hyper-V Virtual Machine

The [Hyper-V Virtual Machine Sensor](#)¹¹³⁰ monitors VMs via Windows Management Instrumentation (WMI) or Windows Performance Counters, as configured in the "Windows Compatibility Options" of the parent device. With this hybrid approach, the sensor first tries to query data via performance counters and uses WMI as a fallback if there are no performance counters available. Performance counters generally need less system resources than WMI. We recommend using System Center Virtual Machine Manager (SCVMM) as parent device for this sensor type, because when your VMs change their physical host with **Live Migration**, this sensor will still be able to continue monitoring. You should also disable User Account Control (UAC) in the Windows operating system of the VM.

Part 11: Sensor Technologies | 10 Monitoring Virtual Environments

The screenshot displays the PRTG Network Monitor interface for a 'Group Hyper-V'. The top navigation bar includes options for Overview, 2 days, 30 days, 365 days, Alarms, Log, Management, Settings, Notification Triggers, Comments, and History. Below the navigation bar, there is a search bar and a status bar showing 62 errors, 1036 warnings, and 19 errors (of 1125). The main content area is organized into a tree view under the 'Hyper-V Group' heading. The tree includes:

- Cluster**: Contains two nodes, 'Larry' and 'Oliver'. 'Larry' has 12 sensors, including PING, Hardware S., Windows C., Windows P., WMI Free D., WMI Memo., CPU: Perce., Broadcom, CPU: Proce., and Memory Pa. 'Oliver' has 6 sensors.
- Hosts**: Contains two nodes, 'Hyper-V 1' and 'Hyper-V 2'. 'Hyper-V 1' has 4 sensors: PING, Hyper-V Ho., HV_Bridged., and Intel[R] Gig. 'Hyper-V 2' has 19 sensors, including Windows and Memory.
- System Center**: Contains two nodes, 'SCVMM' and 'Hyper-V Guests'. 'SCVMM' has 2 sensors: Ping 31 and Host: Hank. 'Hyper-V Guests' has 6 sensors: VM: Aurelio., VM: USATer., VM: V-WBE., VM: V-WBE., VM: V-WBE., and VM: V-WBE.
- Hyper-V Host 1**: Contains 3 sensors: Frank - HV., HV_Bridged., and Intel[R] Gig.

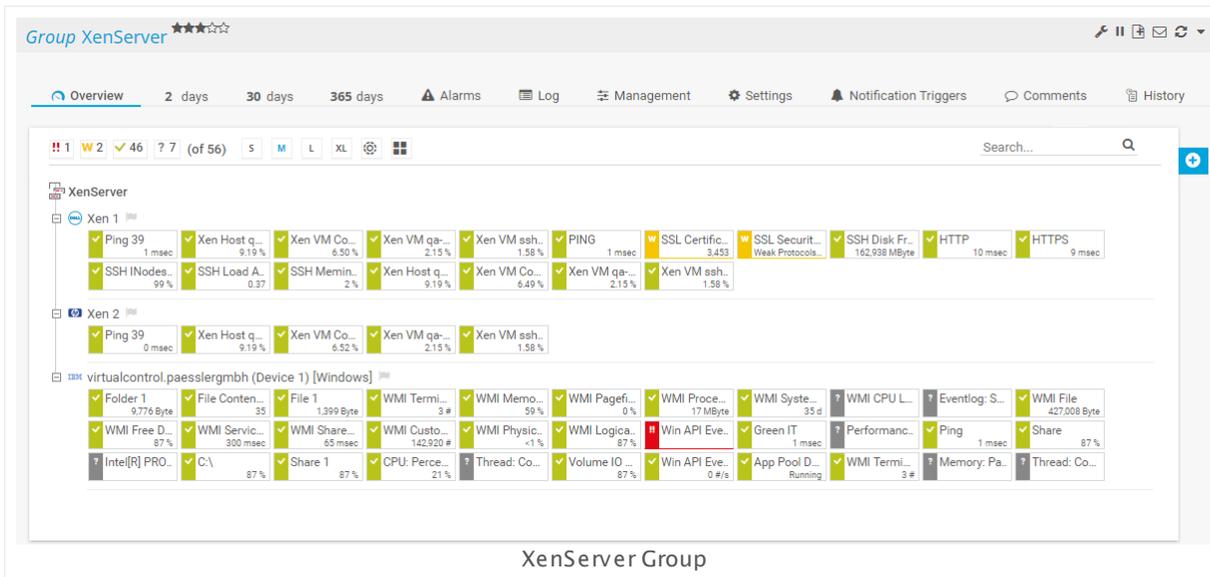
This screenshot shows a sample Hyper-V group in PRTG. There is a dedicated group for failover clustering where two nodes are monitored with several SNMP and WMI sensors, as well as [Hyper-V Host Server sensors](#)^[1121] and sensors for the Hyper-V virtual machines. This ensures that Hyper-V and failover clustering works without any issues. The Hyper-V hosts are monitored the same way, organized in a dedicated group for hosts.

Note that we recommend adding the particular virtual machines to the SCVMM server if possible! We pointed out above that you should add the VMs to an SCVMM server to avoid issues with Live Migration. You can see this in the group "System Center". The particular VMs are added to the dedicated device "Hyper-V Guests".

Citrix XenServer Virtual Machine

The [Citrix XenServer Virtual Machine Sensor](#)^[609] monitors VMs via Hypertext Transfer Protocol (HTTP). For this sensor type, you have to add a device to PRTG that represents a Citrix XenServer with version 5.0 or later. Another requirement is the **Microsoft .NET Framework**: You have to run .NET version 4.5 or later on the probe machine where you add this sensor.

In a XenServer pool, every host knows each running VM. Because of this, there is no central instance that provides all available data, so it does not matter on which host you query your VMs. All queries on any host are automatically forwarded to the pool master, which manages the XenServer pool. So it is sufficient to create the desired sensors for your XenServer VMs on a device that represents one host server of your pool. The XenServer sensors can figure out by themselves which host is running and retrieve the according data.



This screenshot shows a sample XenServer group in PRTG. There are two devices for XenServer hosts (Xen 1 and Xen 2), each with a [Citrix XenServer Host sensor](#)^[599] and several [Citrix XenServer Virtual Machine sensors](#)^[609] for the particular VMs on this host. Furthermore, the Windows operating system is represented as a dedicated device ("virtualcontrol") that is monitored with several WMI sensors regarding CPU, disk, memory, and network usage.

Conclusion

The sensor types described in this section monitor virtual machine specific counters to ensure that all your VMs have enough resources available. If a VM is overloaded, PRTG can notify you immediately and you can proactively take care of issues before a particular VM has an outage or other failures. Additionally, we have shown an idea for a structured virtual monitoring with several recommendations.

 You can find all available sensors for virtual servers and the according virtual machines in section [List of Available Sensor Types—Virtual Servers Sensors](#)^[435].

Performance Considerations

For best performance when monitoring virtual environments, we strongly recommend that you use a computer with **Windows Server 2012 R2** to run the PRTG probe with the according sensors. So for example, you can run up to 300 VMware sensors in a 60-second scanning interval on Windows 2012 R2, while you can only use 30 VMware sensors with the same interval on Windows 2008 R2.

More

Knowledge Base: I run PRTG on VMware. How can I obtain best performance?

- <https://kb.paessler.com/en/topic/49193>

11.11 Monitoring Databases

Monitoring your databases enables you to ensure that, on the one hand, database queries are processed in time, and, on the other hand, that the database itself performs within the defined parameters. Furthermore, database monitoring with PRTG makes it possible to be alerted via a corresponding sensor status if database queries return an unexpected result value.

PRTG comes with built-in native sensors for the most common databases:

- Microsoft SQL servers
- MySQL servers
- PostgreSQL servers
- Oracle SQL servers

It is also possible to monitor many other database servers. For this concern, PRTG uses the ActiveX Data Objects (ADO) interface.

There are two types of database sensors:

- [Sensors monitoring databases directly](#)^[3534]: Monitor databases from the user perspective. These sensors send a request to the database server and receive corresponding values. You can optionally process data tables and show values in individual channels or monitor transactions.
- [Sensors monitoring database performance](#)^[3537]: Monitor databases with a more abstract view on the servers. Usually, these sensors monitor performance counters via Windows Management Instrumentation (WMI).

Sensors Monitoring Databases Directly

PRTG provides several sensors that can "look into" the content of databases. Sensors of this type connect to the database server, execute a defined query, and show the execution time of the whole request and the query. You can use these sensors to process the data table and show requested values in individual channels.

The following sensor types are available for this kind of monitoring:

- [Microsoft SQL v2 Sensor](#)^[1267]: Monitor your Microsoft SQL server 2005 or later.
- [MySQL v2 Sensor](#)^[1284]: Monitor your MySQL server version 5.0 or later.
- [Oracle SQL v2 Sensor](#)^[1457]: Monitor your Oracle database server version 10.2 or later.
- [PostgreSQL Sensor](#)^[1574]: Monitor your PostgreSQL database version 7.x or later.

For these sensor types, you can define valid SQL statements that the sensors send to the database server. Define the queries in an SQL script file and store it into the respective `\Custom Sensors\sql\` subfolder of your PRTG installation (see section [Data Storage](#)^[3734] for details).

You can select this SQL script when you add the sensor to PRTG. With every [scanning interval](#) ³⁴⁵, the sensor executes this script with the defined query against the database and the database returns corresponding values in individual channels (see the [example](#) ³⁵³⁵ below for sample channel value selections). Use the [Sensor Channels Settings](#) ³¹⁶² to define limits for specific values.

i These sensor types need .NET 4.5 or later installed on the computer running the PRTG probe.

Alternatively, you can monitor almost all available database servers with the [ADO SQL v2 Sensor](#) ⁴⁶³ via an ActiveX Data Objects (ADO) connection.

Example: SQL Channel Value Selection

The SQL (v2) sensors determine their channel values by using column numbers, column names, row numbers, or key value pairs. This section shows which option you can choose to get the desired value from an SQL data table.

Consider the following data table that an SQL query might return from a database:

article_id	articles_available	first_listing	orders
00	12	2001	4
01	345	2005	56
02	678	2008	290
03	90	2012	32

This data table has four columns with the following numbering:

- Column 0 has the name "article_id"
- Column 1 has the name "articles_available"
- Column 2 has the name "first_listing"
- Column 3 has the name "orders"

The numbering of columns starts with 0, as well as the numbering for rows starts with 0. The table has four rows, each row contains the properties of one "article". The "articles" have the IDs 00, 01, 02, 03. This also illustrates the proper row numbering (0, 1, 2, 3).

With the options for channel value selection in SQL sensors, you can read out the following values:

- All values that are in row 0 (here: 00, 12, 2001, 4)
- All values that are in column 0 (here: 00, 01, 02, 03)

- All values that are in column 1 (here: 12, 345, 678, 90)

It is not possible to get values from any other cell in a data table. If you need this, you have to re-construct your data table.

The following samples show possible results for channel value selections regarding this data table:

SAMPLE CHANNEL VALUE SELECTIONS

Channel Value Selection by Column Number

This channel will show the value in row 0 of the column you specify. Consider you define "1" as column number. Then the sensor channel value is "12" because it is the cell in column 1 and row 0.

Possible return values for this option are:

- Column number "0" returns "00"
- Column number "1" returns "12"
- Column number "2" returns "2001"
- Column number "3" returns "4"

Channel Value Selection by Column Name

This channel will show the value in row 0 of the column you specify. Consider you define "orders" as column name. Then the channel value is "4" because it is the cell in column "orders" and row 0.

Possible return values for this option are:

- Column name "article_id" returns "00"
- Column name "articles_available" returns "12"
- Column name "first_listing" returns "2001"
- Column name "orders" returns "4"

Channel Value Selection by Row Number

This channel will show the value in column 0 of the row you specify. Consider you define "1" as row number. Then the sensor channel value is "01" because it is the cell in row 1 and column 0.

Possible return values for this option are:

- Row number "0" returns "00"
- Row number "1" returns "01"
- Row number "2" returns "02"
- Row number "3" returns "03"

SAMPLE CHANNEL VALUE SELECTIONS

Channel Value Selection by Key Value Pair This channel will show the value in column 1 of the same row where the key in column 0 was found. Consider you define "02" as key. Then the sensor channel value is "678" because it is the cell in the same row in column 1 as the the key in column 0.

Possible return values for this option are:

- Key "00" returns "12"
- Key "01" returns "345"
- Key "02" returns "678"
- Key "03" returns "90"

This sample channel value selection illustrates how to choose the correct option to get needed values from an SQL data table and shows which cells the SQL sensors can address.

UDF: Counting Returned Rows

If you execute a **UDF (User Defined Function)** on the SQL server and want to know how many rows this UDF returns, follow these steps:

- A command to execute your UDF on the SQL server may look like this, for example:

```
exec myUDF
```

- To get the information how many rows this UDF returns, extend the query in your SQL script:

```
exec myUDF;  
select @@rowcount as row_count
```

- Create a new SQL v2 sensor and enable **Data Processing** during sensor creation.
- In the settings of your SQL sensor, choose the option **Select Channel Value by Column name**
- Enter **row_count** into the **Column Name** field of the channel to show the value from this column in the channel.
- To count table rows returned by a **SELECT** statement, choose the option **Count table rows** in the sensor settings section **Data Processing**.

Sensors Monitoring Database Performance

Performance sensors for database servers have a more "abstract" view on databases and regard performance "from the outside". They do not read out any values of the database, neither do they send SQL queries to databases. This sensor type is only available for Microsoft SQL.

The Microsoft SQL server sensors monitor performance via Windows Management Instrumentation (WMI). You can manually set up different performance counters for your server instances, for example, general statistics, access methods, buffer and memory manager, locks, and SQL statistics.

Microsoft SQL Server performance sensors are available for Microsoft SQL Server 2008, 2012, 2014, 2016, and 2017:

- [WMI Microsoft SQL Server 2008 Sensor](#)  2988
- [WMI Microsoft SQL Server 2012 Sensor](#)  3000
- [WMI Microsoft SQL Server 2014 Sensor](#)  3012
- [WMI Microsoft SQL Server 2016 Sensor](#)  3024
- [WMI Microsoft SQL Server 2017 Sensor](#)  3036

11.12 Monitoring Syslogs and SNMP Traps

PRTG is utilizable as a full-scale syslog server and SNMP trap receiver. Every PRTG installation includes this functionality so no additional software is needed. This manual section describes a sample configuration for PRTG's syslog and SNMP trap receiver and gives you an idea about how to use these features.

Syslog is a well-established standard for computer message logging. Many network devices support sending syslogs to communicate informational, analysis, and debugging messages that are intended for network management and security auditing. SNMP traps are asynchronous notifications from SNMP-enabled devices and can be used to report important incidents and data, just like syslog messages. Devices trigger these messages for various reasons, such as system events, outages, critical conditions, and many more.

PRTG provides two dedicated sensor types that work as full-scale syslog and SNMP trap receivers:

- [SNMP Trap Receiver Sensor](#)  2479
- [Syslog Receiver Sensor](#)  2656

Because both the syslog and the trap receiver are implemented as common sensor types, you do not need to install software in addition to PRTG (for example, you do not need an extra syslog server but only the PRTG web server). You can create the Syslog Receiver as well as the SNMP Trap Receiver sensors in the usual PRTG way via the [add sensor](#)  325 dialog. Then configure your syslog or SNMP trap-enabled device(s) to send messages to PRTG.

Under lab conditions, PRTG could handle about 10,000 syslog and trap messages per second on a quad core desktop machine when using a single sensor without filters.

 The number of messages PRTG can process actually depends on your configuration and system setup. It might be significantly fewer messages.

You can filter the incoming messages by various parameters so that PRTG will process only specific messages and purge other data right away. Processed messages are stored in an internal high-performance database on the particular probe machine and are available for review and analysis via the PRTG web interface. The main limiting factor for storing syslog and trap messages is the hard disk space on the machine running the PRTG probe with these sensors.

Sample Configuration

Follow the steps below for a sample configuration of Syslog and SNMP Trap Receiver sensors. You can apply these instructions to both the SNMP Trap Receiver as well as the Syslog Receiver because the setup works in a similar way for both.

1. [Adding the Receivers](#)  3540
2. [Configure the Source Devices](#)  3541
3. [Collect Messages](#)  3542
4. [Review and Analyze Messages](#)  3544

5. [Refine the Filters](#) ³⁵⁴⁴

6. [Create Notification Triggers](#) ³⁵⁴⁷

Step 1: Add a Syslog Receiver or SNMP Trap Receiver sensor to PRTG.

Both sensor types inherit an implicit filter from the IP address of the parent device. So, on the one hand, it is possible to add these sensors to a [probe device](#) ¹³⁵⁵. Then you will receive all messages from the system running the probe and can optionally filter for specific sources later. On the other hand, you can add these sensors directly to the source device. Then only messages from this device will be processed.

Add the receiver sensors to the desired device in the common way, for example, via the device's [context menu](#) ²⁵⁴¹. We recommend leaving the sensor's default settings unchanged for the first configuration (port, include and exclude filter, warning and error filter) to see what data actually comes in.

i Adding the sensor directly to a network device will increase its speed in comparison to a filter definition in the sensor settings. Distributing Syslog and SNMP Trap Receiver sensors over different probes will make the overall performance scalable and gives you flexibility with the [data storage](#) ³⁷³⁴ location.

i If you do not add the sensor to a probe device but to another device in PRTG, be careful with the configuration: Ensure that the IP address or DNS name of the parent device matches the proper sender. For example, if you want to receive syslog or trap messages from a Storage Area Network (SAN), you might have to add a device to PRTG using the IP address of a specific array member that sends the messages. Providing a DNS name that points to the IP address of a whole group might not work for SANs.

Add Sensor to Device Probe Device [127.0.0.1] (Step 1 of 2)

Monitor What?	Target System Type?	Technology Used?
<input type="radio"/> Availability/Uptime	<input type="radio"/> Windows	<input type="radio"/> Ping
<input type="radio"/> Bandwidth/Traffic	<input type="radio"/> Linux/MacOS	<input type="radio"/> SNMP
<input type="radio"/> Speed/Performance	<input type="radio"/> Virtualization OS	<input type="radio"/> WMI
<input type="radio"/> CPU Usage	<input type="radio"/> Storage and File Server	<input type="radio"/> Performance Counters
<input type="radio"/> Disk Usage		<input type="radio"/> HTTP
		<input type="radio"/> SSH
<input type="radio"/> Memory Usage	<input type="radio"/> Email Server	<input type="radio"/> Packet Sniffing
<input type="radio"/> Hardware Parameters	<input type="radio"/> Database	<input type="radio"/> NetFlow, sFlow, jFlow
<input type="radio"/> Network Infrastructure	<input type="radio"/> Cloud Services	<input type="radio"/> PowerShell
<input type="radio"/> Custom Sensors		<input type="radio"/> Push Message Receiver
		<input type="radio"/> PRTG Cloud

[< Cancel sensor creation](#)
[> Looking for more sensor types? See our PRTG Script World.](#)

Search 1 Matching Sensor Types

Matching Sensor Types

Syslog Receiver ?

Receives and analyzes Syslog messages

Click question mark to open help

+



Looking For More Sensor Types? See our PRTG Script World.

Syslog Receiver Sensor in the Add Sensor Dialog

Step 2: Appropriately configure your network device(s) that support sending syslogs or SNMP traps.

Configure your syslog or SNMP trap ready devices to send syslogs or traps (see the documentation of the respective device vendors). They have to address the PRTG probe where your Syslog or SNMP Trap Receiver sensor runs. So specify the IP address of the machine with the respective PRTG probe. If you keep your syslog or trap receiver's default settings, use the port 514.

- i The protocol is User Datagram Protocol (UDP).
- i The SNMP Trap Receiver does not support **SNMP v3** traps. Please use SNMP v1 or v2c instead.

Filter

Filter are formulas using AND , OR , NOT , brackets and the following fields:

Field	Parameters	Examples
source[ip]	Enter a UDP source IP, IP range, or IP hostmask	source[10.0.23.50] , source[10.0.23.10-50] , source[10.0.23.10/255]
facility[number]	Enter a number or range of the facility code, between 0 and 23	facility[2] , facility[5-7]
severity[number]	Enter a single number or range of the severity code, between 0 (Emergency) and 7 (Debug)	severity[4] , severity[1-3]
hostname[text]	Enter the hostname string to match (exact, case sensitive)	hostname[www.paessler.com]
tag[text]	Enter the tag string to match (exact, case sensitive)	tag[su]
appname[text]	Enter the app name string to match (exact, case sensitive)	appname[myproc]
procid[text]	Enter the process ID string to match (exact, case sensitive)	procid[8710]
msgid[text]	Enter the message ID string to match (exact, case sensitive)	msgid[ID47]
message[parttext]	Enter a substring to match the message field (partial, case insensitive)	message[Error]
data[parttext] data[id,param] data[id,param,value]	Enter a substring to match on structured data as displayed in the table (partial, case sensitive); or enter an ID and a parameter (comma separated) to check if the parameter exists in the ID element; or enter an ID, a parameter, and a value (comma separated) to match on a structured data value (RFC 5424)	data[exampleSDID@32473] , data[exampleSDID@32473,eventSource] , data[exampleSDID@32473,eventSource,Applicati...

Include Filter ⓘ severity[0-6]

Exclude Filter ⓘ

Warning Filter ⓘ severity[4]

Error Filter ⓘ severity[0-3]

Default Sensor Settings: Sufficient for the First Configuration

Step 3: Start collecting syslog or SNMP trap messages from your devices.

You do not have to complete any further configuration steps to use PRTG as a syslog server or SNMP trap receiver. When your device(s) send syslogs or SNMP traps to the specified PRTG probe machine, the messages appear automatically in the PRTG web interface. After each sensor scan (by default, the scanning interval is inherited from the parent device), PRTG will count the received syslogs or traps in the according channels (total number of messages during the last interval, error and warning messages, or dropped packets).

Let the syslog receiver or the SNMP trap receiver collect data for a while to see what comes in. By default, the respective sensor will go into a **Warning** status if there was at least one message with **severity 4** and into an **Error** status if there was at least one message with **severity 3 or lower** during the last sensor scan.

i Incoming messages are counted per scanning interval, so it might take a few moments to see the received syslogs and traps, depending on the remaining time until the next sensor scan. Of course, you can use **Scan Now** via the sensor's [context buttons](#) to perform an immediate scan and see corresponding data. The sensor states are also defined per scan. So, for example, a message that is classified as an error will count for the error channel only for one scanning interval. If there is no new error message in the following scanning interval, no message is shown in the error channel and the error **status** will disappear after the next sensor scan. The syslog or trap itself will still be accessible on the **Messages** tab.

!! Sensor Syslog Receiver 2 ★★★★★
0.02 #/s (Errors) is above the error limit of < 0.01 #/s in Errors

Overview Live Data 2 days 30 days 365 days Messages Historic Data Log Settings

Messages

Drops 0 #/s Errors 0.02 #/s Warnings 0 #/s

0.02 #/s 0 0.02 #/s

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum
Downtime	-4				
Drops	3	0 #	0 #/s	0 #/s	0 #/s
Errors	2	1 #	0.02 #/s	0 #/s	0.02 #/s
Messages	0	1 #	0.02 #/s	0 #/s	0.02 #/s
Warnings	1	0 #	0 #/s	0 #/s	0 #/s

Syslog Messages

Date Time	Source	Message	Hostname	Timestamp	Severity	Tag	Facility	App Name	Proc Id	Msg Id	Data
6/1/201...	127.0.0.1	There is ...	10.0.2.1...	06-01 12...	6	PRTG	19				
6/1/201...	127.0.0.1	There is ...	10.0.2.1...	06-01 12...	6	PRTG	19				
6/1/201...	127.0.0.1	[PRTG N...	10.0.2.1...	06-01 12...	6	PRTG	23				
6/1/201...	127.0.0.1	[PRTG N...	10.0.2.1...	06-01 12...	6	PRTG	23				
6/1/201...	127.0.0.1	[PRTG N...	10.0.2.1...	06-01 11...	6	PRTG	1				
6/1/201...	127.0.0.1	[PRTG N...	10.0.2.1...	06-01 11...	6	PRTG	17				

<< < 0 to 0 > Loading 100%

Syslog Receiver Sensor with Error Messages

Step 4: Review and analyze the collected data.

All incoming messages that match the include filter are processed and stored in the internal high-performance database of PRTG. Review and analyze the received syslogs and traps via the PRTG web interface. For details, see the respective manual sections of [SNMP Trap Receiver Sensor](#)^[2489] and [Syslog Receiver Sensor](#)^[2667]. Then you can decide about further filtering of the incoming messages.

i The received data is also available in the PRTG [data folder](#)^[3734] as common files. One data file is created per hour.

■ In PRTG on premises you can add the Management Information Base (MIB) files of your devices to the `\MIB` subfolder to use them with the SNMP Trap Receiver sensor. This will result in Object Identifier (OID) resolution and makes trap messages more comprehensible. For example, instead of the OID `1.3.6.1.4.1.32446.1.1.2` you would see `SNMPv2-SMI-v1::enterprises.32446.1.1.2 = 0` (example from the PRTG MIB).

Received Syslogs on the Messages Tab

Source	Message	Hostname	Timestamp (Device)	Severity	Tag	Facility	App Name	Procid	Msg Id	Data
6/1/2017 12:44:38 PM	127.0.0.1	There is an emergency issue.	10.0.2.134	06-01 12:44:38	6	PRTG	19			
6/1/2017 12:41:43 PM	127.0.0.1	There is an emergency issue.	10.0.2.134	06-01 12:41:41	6	PRTG	19			
6/1/2017 12:39:18 PM	127.0.0.1	[PRTG Network Monitor	10.0.2.134	06-01 12:39:18	6	PRTG	23			
6/1/2017 12:35:38 PM	127.0.0.1	[PRTG Network Monitor	10.0.2.134	06-01 12:35:38	6	PRTG	23			
6/1/2017 11:24:16 AM	127.0.0.1	[PRTG Network Monitor	10.0.2.134	06-01 11:24:16	6	PRTG	1			
6/1/2017 11:17:32 AM	127.0.0.1	[PRTG Network Monitor	10.0.2.134	06-01 11:17:32	6	PRTG	17			

Step 5: (Optionally) refine the filters.

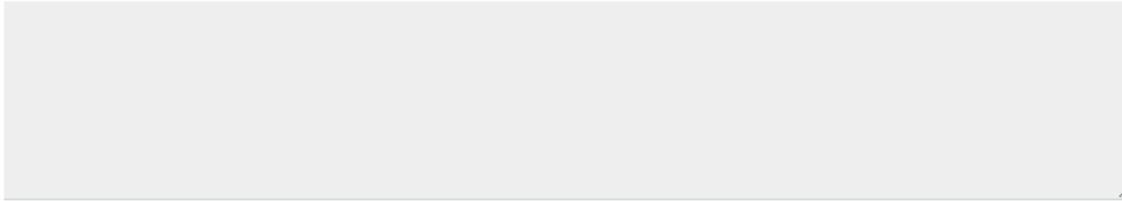
In order to increase productivity with your PRTG syslog servers and trap receivers, you can adjust the default filter settings. PRTG provides a comprehensible formula system that you can use to describe what kind of messages you want to process and which of them will count as error or warning messages. You can configure the following filters for received messages in the settings of the respective receiver:

- **Include filter:** Process and store specific types of messages only.
- **Exclude filter:** Do not process specific types of messages and discard them.
- **Warning filter:** Define rules to categorize received messages as warnings.
- **Error filter:** Define rules to categorize received messages as errors.

Use the syntax that is provided in the corresponding manual sections to define your individual filter rules: [SNMP Trap Receiver Sensor](#)²⁴⁸⁸ and [Syslog Receiver Sensor](#)²⁶⁶⁵.

 You can create filter rules with a few mouse clicks in the **Advanced Filter** on the **Messages** tab of a specific sensor and copy these rules into the sensor settings to apply them.

Advanced Filter



Filter are formulas using AND , OR , NOT , brackets and the following fields:

Field	Parameters	Examples
source[ip]	Enter a UDP source IP, IP range, or IP hostmask	source[10.0.23.50] , source[10.0.23.10-50] , source[10.0.23.10/255]
facility[number]	Enter a number or range of the facility code, between 0 and 23	facility[2] , facility[5-7]
severity[number]	Enter a single number or range of the severity code, between 0 (Emergency) and 7 (Debug)	severity[4] , severity[1-3]
hostname[text]	Enter the hostname string to match (exact, case sensitive)	hostname[www.paessler.com]
tag[text]	Enter the tag string to match (exact, case sensitive)	tag[su]
appname[text]	Enter the app name string to match (exact, case sensitive)	appname[myproc]
procid[text]	Enter the process ID string to match (exact, case sensitive)	procid[8710]
msgid[text]	Enter the message ID string to match (exact, case sensitive)	msgid[ID47]
message[parttext]	Enter a substring to match the message field (partial, case insensitive)	message[Error]
data[parttext] data[id,param] data[id,param,value]	Enter a substring to match on structured data as displayed in the table (partial, case sensitive); or enter an ID and a parameter (comma separated) to check if the parameter exists in the ID element; or enter an ID, a parameter, and a value (comma separated) to match on a structured data value (RFC 5424)	data[exampleSDID@32473] , data[exampleSDID@32473,eventSource] , data[exampleSDID@32473,eventSource,Application]

OK

Cancel

Advanced Filters on the Messages Tab

Step 6: (Optionally) create notification triggers.

By default, the warning and error channels of the Syslog and SNMP Trap Receiver sensors have a very low upper warning or error limit (0.00000001). The reason for this is that even when only one syslog or trap has been counted in the respective channel during a scanning interval, the overall status of the sensor will show this with the corresponding status. This way, you always recognize if there is something wrong on the monitored system.

Because of this sensor behavior, best practice would be to add a **State Trigger** on the **Notification Triggers**^[3216] tab of the sensor if you want to get a **notification**^[143] when a warning or error message type comes in. Define **0 seconds Down** or **Warning** time condition to not miss any warnings, errors, or any other messages. Another option would be a **Speed Trigger** for notifications regarding messages per second.

See also this Knowledge Base article: [How can I configure sensors using speed limits to keep the status for more than one interval?](#)

You can use syslog and trap specific placeholders in notification templates in order to see the messages when you receive a notification. See the **More**^[3547] section below for more information.

The screenshot shows the 'Notification Triggers' configuration page for a 'Sensor Syslog Receiver'. The 'Notification Triggers' tab is active, and a 'State Trigger' is configured. The rule is: 'When sensor state is Down for at least 0 seconds perform Ticket Notification (paused)'. The '0 seconds' value is circled in red. Below this, there are options for 'and repeat every 0 minutes' and 'When condition clears after a notification was triggered perform no notification'.

More

Knowledge Base: How can I configure sensors using speed limits to keep the status for more than one interval?

- <https://kb.paessler.com/en/topic/73212>

Knowledge Base: What placeholders can I use with PRTG?

- <https://kb.paessler.com/en/topic/373>

11.13 Monitoring via Push

PRTG provides the option to monitor passively received data. For this purpose, you can set up a device in a way that it automatically sends the data to PRTG. Specific sensor types can receive this data and alarm you based on your individual settings. For example, all Linux/Unix and most network devices support remote devices generating data, which has to be configured on each device, and sending the messages to a PRTG probe system. Usually, only the destination IP and port are required.

Push monitoring enables you to use webhooks to push messages to the PRTG server using Hypertext Transfer Protocol (HTTP). Wikipedia describes a webhook as a method of augmenting or altering the behavior of a web page or application with custom callbacks.

PRTG comes with built-in sensor types for push monitoring:

- [HTTP Push Count Sensor](#)^[1046]: counts the number of received messages.
- [HTTP Push Data Sensor](#)^[1056]: displays numerical values from received messages.
- [HTTP Push Data Advanced Sensor](#)^[1070]: shows received values and messages encoded in valid XML or JSON.

Use Cases

The push technology can be useful for monitoring in different cases, for example when target devices do not allow requests via the usual technologies. The following scenarios are good examples of where to use HTTP Push sensors.

- Devices that cannot run a PRTG probe
- Appliances that are not accessible via SSH or SNMP
- Web servers that can run certain scripts or PHP periodically
- Migrating a lot of EXE sensors into one EXE script that manages the HTTP Push sensors and sends data to them. Some coding is required, see this Knowledge Base article: [How can I monitor SCVMM hosts and VMs with PRTG?](#)
- When monitoring Linux services, see this Knowledge Base article: [How can I monitor and automatically restart a service on a Linux host?](#)
- If you need to push **a lot** of data into PRTG in short periods of time; the sensors have been tested with about 10,000 values pushed within one minute.

How to Use

Webhooks basically work like push messages. These are triggered by an event (for example, a new comment to a blog post) and send according information in real time to a specified URL. You can use this technology to push messages to the PRTG Probe, and monitor count and content with HTTP Push sensors. Because webhooks use HTTP, you can integrate them without having to add new infrastructure to your network.

Recommended Configuration

Follow the steps below for a sample configuration of the HTTP Push sensors.

1. Add the sensors.
2. Define the URLs.

Step 1: Add the HTTP Push Count, HTTP Push Data, and HTTP Push Data Advanced sensors to PRTG.

You can use the standard method to add sensors to your configuration.

1. Choose the Probe Device or a device of your own.
 -  A device of your own has no practical advantage with HTTP Push sensors but it might help you stay better organized.

2. Click **Add Sensor** and filter for **Push Message Receiver** under **Technology Used**.

3. Select one of the HTTP Push sensors that fits best to your intended usage.

 For more details, see section [Add a Sensor](#)³²⁵.

 These sensor types cannot be used in cluster mode. You can set them up on local probes or remote probes only, not on cluster probes.

Step 2: Define the corresponding URL to send HTTP requests to PRTG.

In order for the desired configuration to be properly sent to and received by PRTG, please use the following URL formats.

The **HTTP Push Count Sensor** uses the following URL:

`http://<probe_ip>:<port_number>/<token>`

Replace the parameters `<probe_ip>`, `<port_number>`, and `<token>` with the corresponding values.

- The `<probe_ip>` is the IP address of the system where the PRTG probe with the sensor is running.
- The `<port_number>` is where the sensor listens for incoming HTTP calls.
- The `<token>` is used to define the matching sensor.

Example:

```
http://192.0.2.0:5050/XYZ123
```

 You can use several sensors with the same port and identification token. In this case, the number of push messages will be shown in each of these sensors.

The **HTTP Push Data Sensor** uses the following URL:

http://<probe_ip>:<port_number>/<token>?value=<integer_or_float>&text=<text message>

Replace the parameters **<probe_ip>**, **<port_number>**, **<token>**, and **<integer_or_float>** with the corresponding values. The **&text** parameter is optional: You can omit it.

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running.
- The **value** can be an integer or a float value, depending on the data of your application; you have to set the value type accordingly in the sensor settings. This parameter will be the sensor value.
 - ⚠ If this parameter is missing, the sensor will show a **down** status.
- You can **optionally** add a custom text message by replacing the parameter **<text message>** with it. The text will be shown as sensor message. If there is no value but only a text, the text will be shown as error message.
 - ⚠ This text message has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Example:

```
http://192.0.2.0:5050/XYZ123?value=0&text=this%20is%20a%20message
```

- ⓘ You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

The **HTTP Push Data Advanced Sensor** uses the following URLs depending on the type of HTTP request.

- **GET requests:** **http://<probe_ip>:<port_number>/<token>?content=<valid XML_or_JSON>**

The XML encoded value of the content parameter has to match the format as defined in section [Custom Sensors](#)³⁶⁴¹.

- **POST requests:** **http://<probe_ip>:<port_number>/<token>**

This HTTP request method sends the XML or JSON encoded HTTP body as POST data. The body has to match the format as defined in section [Custom Sensors](#)³⁶⁴¹. We strongly recommend the HTTP content type **application/xml** or **application/json**.

Replace the parameters **<probe_ip>**, **<port_number>**, **<token>**, and **<valid XML_or_JSON>** (for GET requests) with the corresponding values:

- You can define **port number** and **identification token** in the sensor settings.
- The **probe IP** is the IP address of the system on which your PRTG probe with this sensor is running.
- The content of GET requests has to be valid XML or JSON in the PRTG API format.
 - ⚠ The content has to be URL encoded (for example, the whitespaces in the sample URL below); most browsers achieve this automatically.

Minimum example for the GET method that returns one static channel value:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10</value></result><
```

⚠ By default, values within the `<value>` tags in the returned XML or JSON must be **integers** to be processed. If **float** values are returned, you have to explicitly define this value type as defined in section [Custom Sensors](#) with `<float>` tags, otherwise the sensor will show **0** values in affected channels. Example:

```
http://127.0.0.1:5050/XYZ123?content=<prtg><result><channel>MyChannel</channel><value>10.45</value><float>
```

i You can use several sensors with the same port and identification token. In this case, the data of push messages will be shown in each of these sensors.

Conclusion

These sensor types are great tools to count and display HTTP push messages to the PRTG server and to keep you up-to-date with real-time information about your network.

More

Knowledge Base: How can I monitor SCVMM hosts and VMs with PRTG?

- <https://kb.paessler.com/en/topic/68767>

Knowledge Base: How can I monitor and automatically restart a service on a Linux host?

- <https://kb.paessler.com/en/topic/70771>

11.14 Monitoring via HTTP

The Hypertext Transfer Protocol (HTTP) is a standard application layer protocol and the basis for data communication in the internet. HTTP is a request-response method for client-server architectures, where the client sends a request and the server processes and responds to the request.

Monitoring via HTTP is useful if you want to monitor websites or web servers. It enables you to keep an eye on the availability and download times of a website or the performance statistics of a web server. There are also a lot of other possible use cases for HTTP sensors. For example, you can request any Application Programming Interface (API) that is reachable via HTTP and monitor returned values. This approach makes it possible to include almost any type of device or application into your monitoring.

PRTG comes with built-in sensor types for HTTP monitoring:

- [Cloud HTTP Sensor](#)  619
- [Common SaaS Sensor](#)  644
- [HTTP Sensor](#)  955
- [HTTP Advanced Sensor](#)  965
- [HTTP Apache ModStatus PerfStats Sensor](#)  982
- [HTTP Apache ModStatus Totals Sensor](#)  992
- [HTTP Content Sensor](#)  1002
- [HTTP Data Advanced Sensor](#)  1014
- [HTTP Full Web Page Sensor](#)  1027
- [HTTP Push Count Sensor](#)  1049
- [HTTP Push Data Sensor](#)  1059
- [HTTP Push Data Advanced Sensor](#)  1070
- [HTTP Transaction Sensor](#)  1081
- [HTTP XML/REST Value Sensor](#)  1095
- [REST Custom Sensor](#)  1646

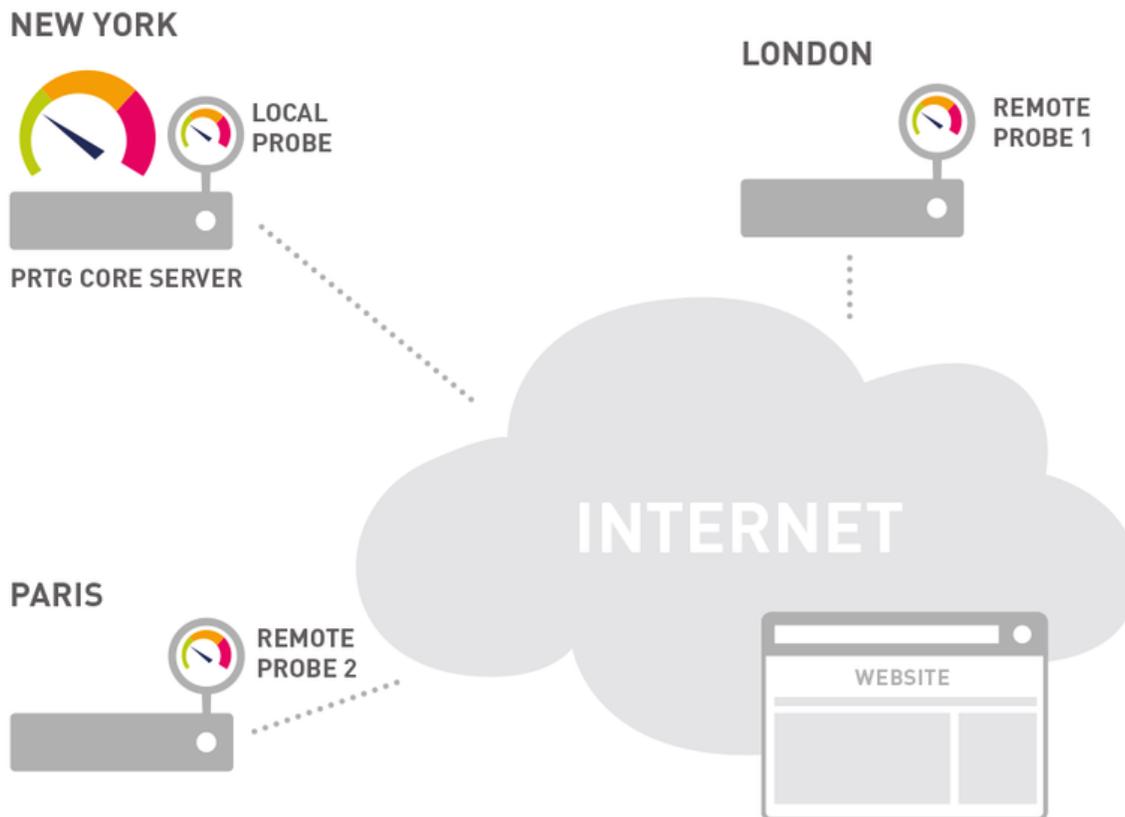
Use Cases

- Monitor the availability and loading times of a website
- Monitor the source code and specific content of a website
- Test the login, purchasing, and shipping processes of a web shop
- Monitor performance statistics and activity of Apache web servers

Types of HTTP Monitoring

Availability Monitoring

This type monitors the availability of a website or a specific website element. For example, the [HTTP sensor](#)^[955] shows how long the HTML code of a website takes to load. If the sensor shows a loading time that is much longer than expected, then the website may not be responding or may be unavailable.



Cloud HTTP Monitoring Provides Better Performance Statistics

The HTTP sensor uses different HTTP requests to request the given URL.

- **GET:** requests the website directly
- **POST:** sends post form data to the URL
- **HEAD:** requests the HTTP header only, without the actual webpage body, saving bandwidth

The [HTTP Advanced sensor](#)^[965] also monitors the availability of a website, along with other parameters such as bytes received, download bandwidth (speed), and time to first byte, which shows you how fast your web server responds. This sensor lets you use a (custom) user agent when connecting to the target URL and lets you send custom HTTP headers to the target URL.

The [Cloud HTTP sensor](#)^[619] monitors a web server from various locations across the globe. For example, the URL of a website to measure the loading time of a page's source code or the URL of a page asset to measure its availability and loading time. It also shows the global average response time.

The [Cloud Ping sensor](#)^[629] also monitors the availability of your website.

The [Common SaaS sensor](#)^[644] monitors the availability of your cloud services and is an important pillar for unified monitoring.

Content Monitoring

This type monitors internal values of a web server based application or changes to specific content on a website. The [HTTP Full Web Page sensor](#)^[1027] measures the time it takes to download a webpage including all embedded page elements, such as Flash content, images, etc.

i This monitoring option can create a lot of bandwidth traffic, depending on the page size and the scanning interval.

Additionally, the [HTTP Content sensor](#)^[1002] monitors a numerical value returned by an HTTP request. A 'change' notification can optionally be triggered to notify you of changes to the content.

Example: Content Monitoring

■ For example, consider a URL <http://www.example.com/status.html> that returns a PHP script with the current system status in a simple HTML page.

```
<html>
<body>
  Description: Script gives back current status of disk free (%) and CPU usage (%).
  [85.5][12.0]
</body>
</html>
```

You would configure the HTTP Content sensor using

- the script **URL** from above,
- value type **Float**,
- and number of channels **2**.

The sensor calls the URL with every scanning interval and only regards the two values in square brackets `[]`, handling each of them in one sensor channel. The additional description text and HTML tags are not necessary. In this example, they are added in case a human calls the URL.

i If you define the number of channels as **1**, the sensor will read only the first value. The second value will be ignored. Using **3** as number of channels will result in a sensor error message.

To be notified when the website content changes, you first need to configure a **Trigger 'change notification'** in the sensor's settings and then the notification itself.

See section [Sensor Notification Triggers Settings](#)^[3180] for more information.

Performance Monitoring

The HTTP Transaction sensor checks if a web shop is working as expected: with a series of requests, you can simulate the login, purchasing, and shipping processes, for example. Only if all actions can be completed successfully in a row, the check returns an "OK" message. If anything goes wrong, you are immediately alerted and can react instantly to avoid loss of earnings for your company because the web shop is unavailable or very slow.

Apache Web Server Monitoring

The HTTP Apache ModStatus PerfStats and HTTP Apache ModStatus Totals sensors monitor performance statistics and the activity of an Apache web server using `mod_status` over HTTP. Among other HTTP sensors, these sensors allow you to enter credentials for webpages that need authentication and allow you to choose the necessary authentication method.

Security Monitoring

PRTG also provides the option to monitor the security of your website by checking the status of SSL certificates and the security of a connection.

- **SSL Certificate Sensor:** monitors the certificate of a secure SSL/TLS connection. It displays whether a certificate has been revoked, or is trusted as root authority, or is self-signed, for example.
- **SSL Security Check Sensor:** monitors the SSL connectivity to the port of a device. It tries to connect to the specified TCP/IP port number of a device with various SSL/TLS protocol versions and shows if a specific protocol is supported.

Push Monitoring

PRTG provides the option to monitor passively received data. For this purpose, you can set up a device in a way that it automatically sends the data to PRTG. Specific sensor types can receive this data and alarm you based on your individual settings. For example, all Linux/Unix and most network devices support remote devices generating data, which has to be configured on each device, and sending the messages to a PRTG probe system. Usually, only the destination IP and port are required.

See section [Monitoring via Push](#)^[3548] for more information.

Other Data

You can also monitor other types of data from your website, for example the number of website visitors via the [HTTP XML/REST Value sensor](#)^[1095]. The sensor lets you monitor values within the returned XML code, provided your web analytics tool has an XML export option. The [HTTP Data Advanced sensor](#)^[1014] access a web server and retrieves XML or JSON encoded data.

The [REST Custom sensor](#)^[1646] queries a REST Application Programming Interface (API) endpoint and maps the JSON or XML result to sensor values. The mapping rule has to be available as a REST configuration file in JSON template (*.template) format according to the API definition.

 For details about the return value format, see section [Custom Sensors](#)³⁶⁴¹.

HTTP Status Codes

The HTTP sensors show their status depending on the HTTP status codes that they receive. By default, the sensor states are the following:

HTTP STATUS CODE	HTTP SENSOR STATUS
2xx Success	Up (Green)
3xx Redirection	Warning (Yellow, Down (Red) for too many redirects)
4xx Client Error	Down (Red)
5xx Server Error	Down (Red)

 You need to configure your HTTP sensor(s) manually only if you want to change these default reactions. In this case, you can change the sensor status based on limits and/or keyword checks.

Other HTTP Sensor Settings

- **Server Name Identification (SNI):** You can configure SNI, which has to be a Fully Qualified Domain Name (FQDN) and must match the configuration of the target server. For details, see the Knowledge Base article [My HTTP sensors fail to monitor websites which use SNI. What can I do?](#)
- **Protocol Version:** You can choose the HTTP protocol version that the sensor will use when connecting to the target URL.
- **Authentication Method:** You can define if the configured URL needs authentication, enter credentials, and choose an authentication method.
- **Custom User Agent:** You can enter a string to be used as user agent when connecting to the target URL.
- **Custom HTTP Headers:** You can send custom HTTP headers to the target URL.

HTTP Sensor Troubleshooting

See the following Knowledge Base articles for troubleshooting and other tips for monitoring with HTTP sensors.

- [Which user agent should I use in the HTTP Advanced sensor's settings?](#)

- [HTTP Full Web Page sensor is “unable to navigate”. What can I do?](#)
- [What to do when I see a CreateUniqueTempDir\(\) error message for my HTTP Full Webpage Sensor?](#)
- [Where can I find more information about the HTTP XML/REST Value Sensor?](#)
- [Why does my HTTP XML/REST Value sensor return a 404 error?](#)
- [My HTTP sensors could not create an SSL secure channel and are down. What can I do?](#)

Conclusion

These sensor types are great tools to monitor your website's availability and performance and to keep you up-to-date with real-time information.

More

Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

- <https://kb.paessler.com/en/topic/65731>

Knowledge Base: My HTTP sensors fail to monitor websites which use SNI. What can I do?

- <https://kb.paessler.com/en/topic/67398>

Knowledge Base: Which user agent should I use in the HTTP Advanced sensor's settings?

- <https://kb.paessler.com/en/topic/30593>

Knowledge Base: How can I monitor internal values of a web application with PRTG?

- <https://kb.paessler.com/en/topic/4>

Knowledge Base: What is the difference between "HTTP" and "HTTP Full Web Page" Web Server sensors?

- <https://kb.paessler.com/en/topic/943>

Knowledge Base: Configuration Tips for HTTP Transaction Sensors needed

- <https://kb.paessler.com/en/topic/443>

Knowledge Base: Is there a tool available that can help me building queries for the XML/Rest Sensor?

- <https://kb.paessler.com/en/topic/48783>

Part 12

PRTG Administration Tool

12 PRTG Administration Tool

The **PRTG Administration Tool** is part of your PRTG installation and helps you edit administrative settings of your local probe and your remote probe installations.

You can launch the PRTG Administration Tool from the Windows start menu, on your core server, or on your remote probe server. If you start the PRTG Administration Tool on the PRTG core server, you can change settings that affect your whole PRTG installation and your local probe. If you run the PRTG Administration Tool on a system on which a remote probe runs, you can only change settings that are related to this probe.

All settings that you change will require a restart of the affected PRTG Windows services to apply any changes on the configuration. See the following sections for details.

i You can also change many administrative settings via the [Setup](#)³³⁰² in the [PRTG web interface](#)¹⁶⁶⁶. For probes, settings are also available on the [corresponding tab](#)³⁷¹¹ in the web interface.

i You can review the history of all changes to the settings of the PRTG Administration Tool in the **Logs (Debug)** directory. The name of the corresponding logfile is **PRTG Administration Tool Changelog.log**. For information on how to find the folder used for storage, see section [Data Storage](#)³⁷³⁴.

More

Video Tutorial: The PRTG Administration Tool

- <https://www.paessler.com/support/videos/prtg-basics/administration-tool>

PRTG Administration Tool—Topics

- [PRTG Administration Tool on Core Server System](#)³⁵⁶¹
- [PRTG Administration Tool on Remote Probe System](#)³⁵⁸⁷

Related Topics

- [Setup](#)³³⁰²
- [Failover Cluster Step by Step](#)³⁷²⁷

12.1 PRTG Administration Tool on Core Server System

With the **PRTG Administration Tool** you can define various system-oriented settings that affect your PRTG installation, as well as restart services and view log information. You can also change many of these settings via the [system administration](#)^[3302] in the [PRTG web interface](#)^[168].

i This section describes the available settings in the PRTG Administration Tool when you open the tool on the **PRTG core server system**. This means that you can edit settings that regard your PRTG core or web server and the local probe, which is the probe on your core server. If you open the PRTG Administration Tool on a remote probe machine, only [probe related settings](#)^[3587] are available.

i All settings you define are only valid for the local installation that is running on the computer on which you start the Administration Tool. In order to change settings for another installation, for example, another cluster node installation, please log in to that computer and open the program there.

i Do you want to know how the PRTG Administration Tool relates to all other major parts of PRTG Network Monitor? To get familiar with the different components of PRTG, we recommend that you read the [Architecture](#)^[125] section. If you prefer a video introduction to the **PRTG Administration Tool**, see the [More](#)^[3586] section below for more information.

 This feature is not available in PRTG hosted by Paessler.

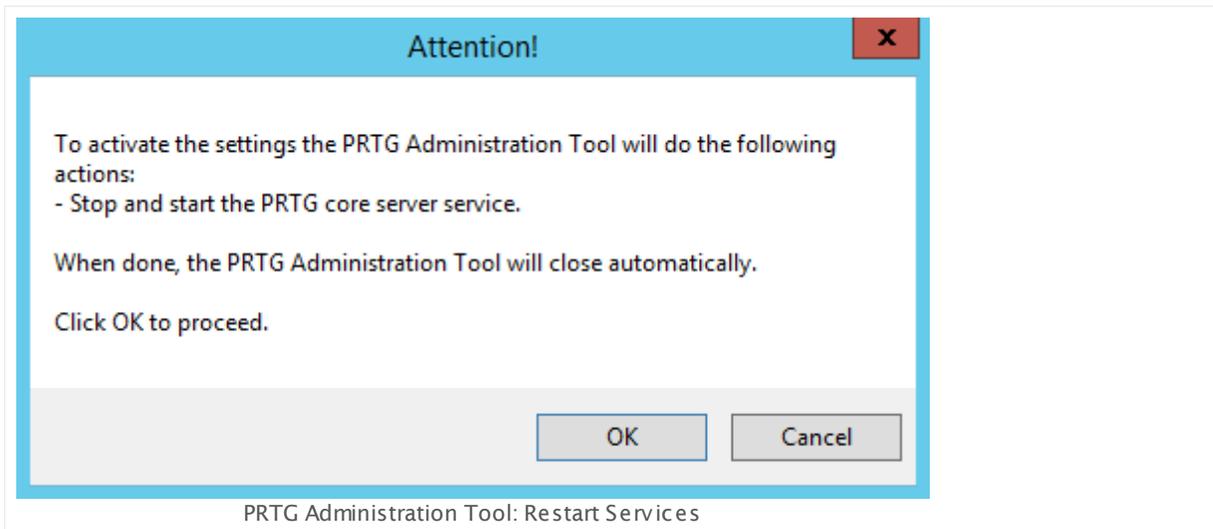
Start the PRTG Administration Tool

From the Windows start menu, select the **PRTG Network Monitor** group and click **PRTG Administration Tool** to open the application.

You can choose from these options in different tabs:

- [Web Server](#)^[3562]
- [Core Server](#)^[3566]
- [Cluster](#)^[3568]
- [Administrator](#)^[3574]
- [Probe Settings for Core Connection](#)^[3575]
- [Probe Settings for Monitoring](#)^[3579]
- [Service Start/Stop](#)^[3580]
- [Logs and Info](#)^[3583]

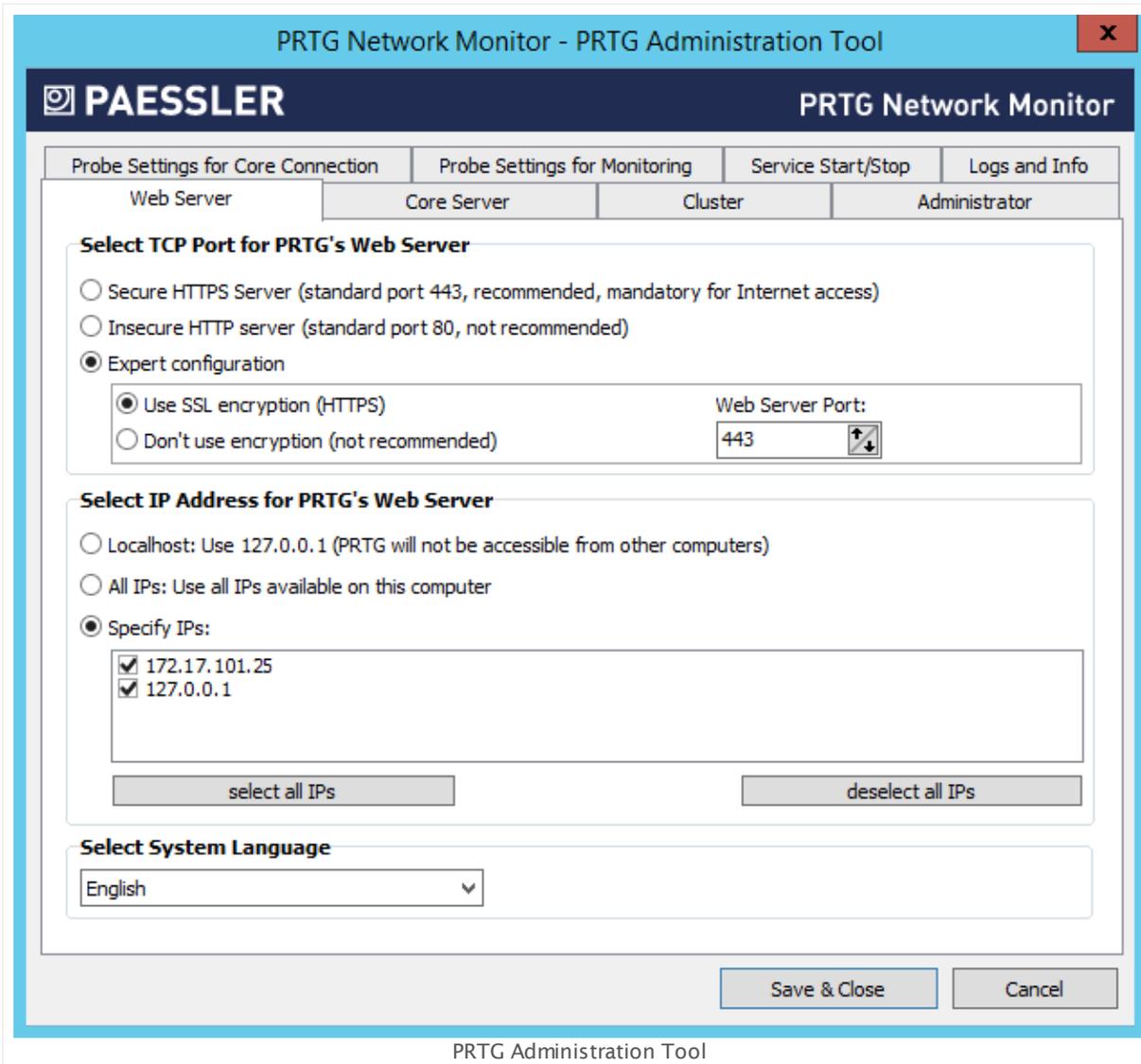
After you change settings, click the **Save & Close** button. A new window opens where PRTG asks you to agree to restart the PRTG core server service. Click **OK** if you do not want your changes to be ignored.



Web Server

Edit IPs, ports, access methods, and language for the [PRTG web interface](#)¹⁶⁶.

i You can also change all settings on the **Web Server** tab via the PRTG web interface in the [User Interface](#)³³⁴³ settings.



WEB SERVER

Select TCP Port for PRTG's Web Server

PRTG runs a web server in order to provide access via the web interface and the Enterprise Console. Please specify on which port this web server will run. Choose between:

WEB SERVER

- **Secure HTTPS server (recommended, mandatory for internet access):** We recommend this setting and you need it to access the PRTG server via the internet. Use a secure HTTPS connection that is encrypted via SSL on port 443.

 Although the connection is secure, you will see an [SSL Certificate Warning](#)^[172] in your browser when logging in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[376].

 If port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will then be redirected to port 443 via HTTPS. You can change this behavior by using a registry setting.

If port 443 is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG will send a [ticket](#)^[230] that shows you the currently used port number and will switch back to 443 as soon as it is available again.

- **Insecure HTTP server (standard port 80, not recommended):** Use a standard web server without SSL encryption on port 80. This setting is not recommended for WAN connections.
 -  If you use an insecure web server on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

- **Expert configuration:** This setting allows you to specify a custom web server port and the security of the connection. This option is intended for systems with an existing web server on the standard port. Define port and encryption below.

 If PRTG always uses a fallback port after a server restart, check for other programs that use the same port as PRTG. For example, the Microsoft IIS web server also uses the port 80 (443 for SSL) by default and blocks it. Please disable such programs and services on startup.

Expert Configuration:
SSL Encryption

You will see this setting only if you select **Expert configuration** above. Specify if you want to use an SSL encryption. Choose between:

- **Use SSL encryption (HTTPS):** Use a secure HTTPS connection that is encrypted via SSL on a custom port as defined above.
 -  Although the connection is secure, you will see an [SSL Certificate Warning](#)^[172] in your browser when you log in to the PRTG web interface, because the default certificate is unknown to your browser. You can install another SSL certificate for PRTG later. Please see [Using Your Own SSL Certificate](#)^[376].

WEB SERVER

- **Don't use encryption (not recommended):** This setting is not recommended for WAN connections. Use a standard web server without SSL encryption on a custom port as defined above.

 If you use a web server without encryption on the internet, attackers could potentially spy on credentials you enter into PRTG. We strongly recommend that you use this option in a LAN only.

Expert Configuration: Web Server Port

You will see this setting only if you select **Expert configuration** above. Enter the TCP port number you want the PRTG web server to run on. Please enter an integer value.

 If you use a secure connection and port 80 is free, PRTG will reserve it as well. When users try to connect on port 80 via HTTP, they will be redirected to the custom port via HTTPS. You can change this behavior by using a registry setting.

 If the defined port for a secure connection is not available, PRTG will try port 8443 as fallback. If this port is also not available, PRTG searches from port 32000 upwards for a free port. PRTG sends a [ticket](#)²³⁰¹ that shows you the currently used port number and will switch back to the original port as soon as it is available again.

Select IP Address for PRTG's Web Server

PRTG is running a web server in order to provide access via the web and Windows interface. Please specify the IP address this web server will run on. Later, you can log in to PRTG by simply pointing your browser to the specified IP address.

Choose between:

- **Localhost, 127.0.0.1 (PRTG will not be accessible from other computers):** Use **127.0.0.1** only. The PRTG web interface and the Enterprise Console will only be accessible from the computer PRTG is installed on. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on **127.0.0.1**.

 If you run PRTG on localhost, please do not use the DNS name **http://localhost** to log in to the web server, as this may considerably slow down the PRTG web interface. Please use your local IP address or **http://127.0.0.1** instead.

- **All IPs available on this computer:** Use all IP addresses available on this computer and enable access to the web server for all of these addresses. The TCP port selected below must be free on every available IP address.

WEB SERVER

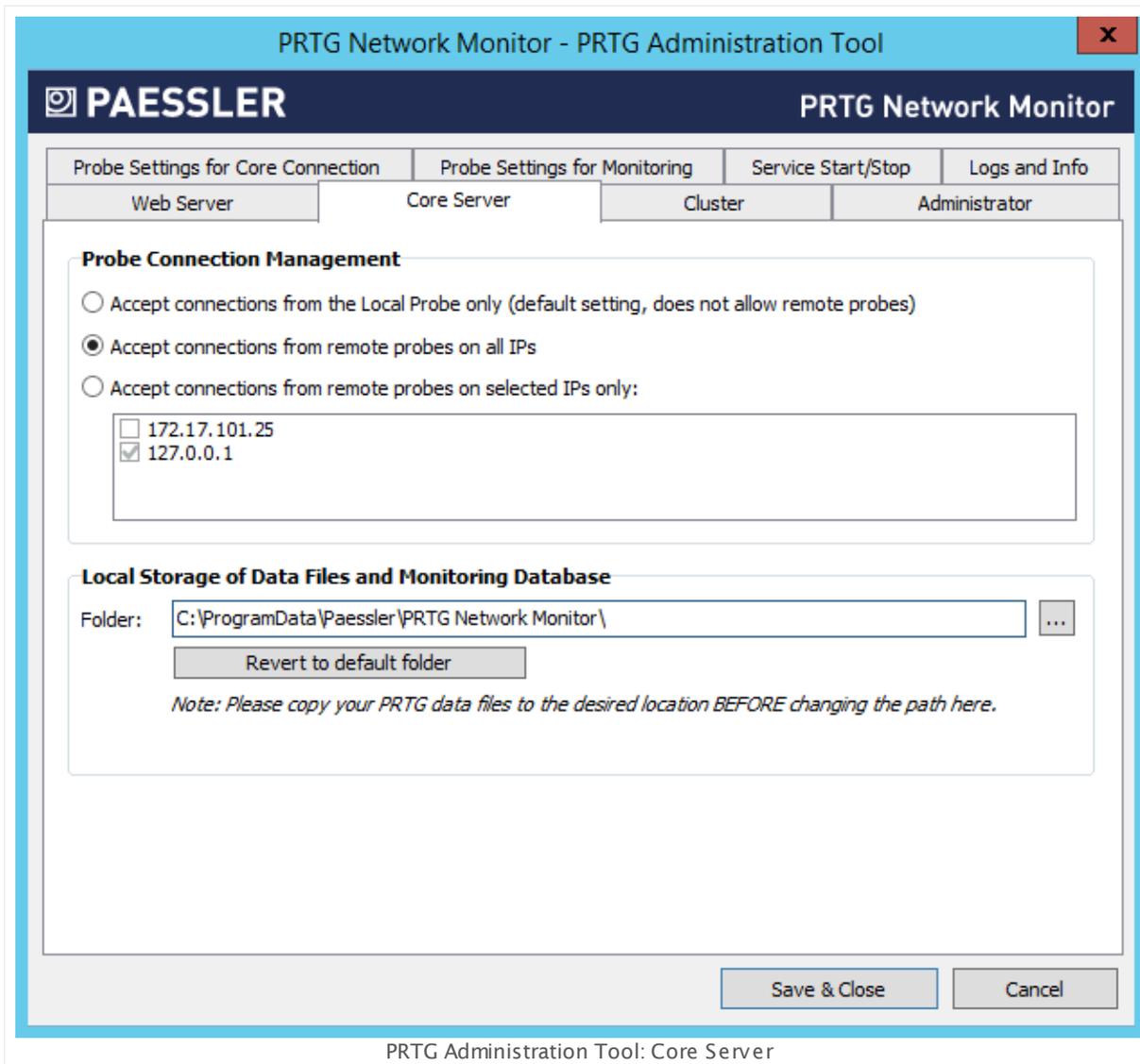
- **Specify IPs:** Select specific IP addresses on which the PRTG Web server will run. A list specific to your system is shown. Add a check mark in front of every IP address you want the PRTG web server to be available at. You can also select and deselect all addresses by clicking on the check box in the table header. Either the selected port or at least one port in the range from **8080** to **8089** has to be available on the specified IP address.
- ❗ Regardless of the selected setting above, one port in the range from **8080** to **8180** has to be available on the specified IP address so PRTG can create reports. The report engine will try to connect to the core server on one of these ports.
- ❗ If PRTG does not find a network card on startup it will switch the IP setting to **Localhost**. This setting will remain, even if a network card is available later on. If you disabled or removed the network card on the machine running the PRTG core server, please re-check this setting.

Select System Language

Choose the system language from the dropdown list. Default is **English**. Depending on your installation, you may be able to choose other languages here. This setting defines the language of the [PRTG web interface](#)¹⁶⁶, as well as of the [PRTG Administration Tool](#)³⁵⁶.

Core Server

Define settings for the core server.



CORE SERVER

Probe Connection Management

Define how PRTG will handle incoming connections from probes. Choose between the following options:

- **Accept connections from the Local Probe only (default setting, does not allow remote probes):** This is the default setting. Only local probe connections will be accepted by the PRTG core server. You cannot use [remote probes](#) with this setting enabled.
- **Accept connections from remote probes on all IPs:** Incoming connections from remote probes will always be accepted, no matter on which IP address of the core server they come in.

CORE SERVER

- **Accept connections from remote probes on selected IPs only:** Incoming connections from [remote probes](#)³⁷¹⁹ will only be accepted on the selected IP address(es) of the core server. In the list, select the IP addresses by adding a check mark in front of the desired IPs.

You can also change this setting in the PRTG web interface under [System Administration—Core & Probes](#)³³⁰⁹.

Local Storage of Data Files and Monitoring Database

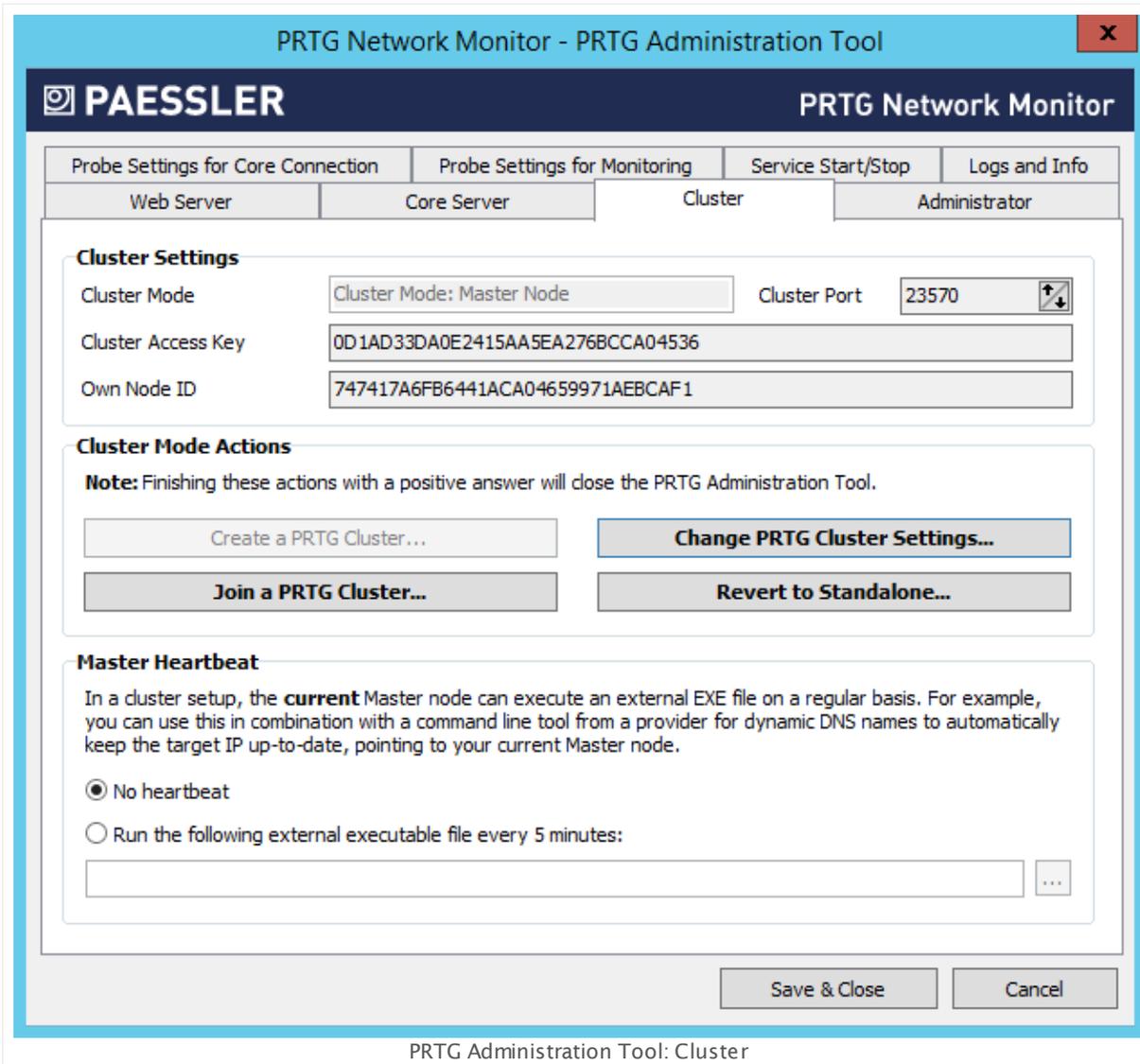
Define the data folder to which PRTG will store configuration and monitoring data. Click the ... button to choose another folder on your system.

 Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location.

Click **Revert to default folder** to reset to default.

Cluster

On the **Cluster** tab, you can manually change how the current core installation will behave in a cluster. Before changing settings here, please read the [Failover Cluster Configuration](#)³⁷²⁰ section.



CLUSTER

Cluster Settings

Depending on the current cluster settings, you will see different information here.

- **Cluster Mode:** Shows which cluster mode the current installation is running. This setting is shown for your information only and cannot be changed here. Possible values are **Standalone** (no cluster mode), **Cluster Mode: Master Node**, or **Cluster Mode: Failover Node**.
- **Cluster Port:** This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.

CLUSTER

- **Cluster Access Key:** This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.
- **Own Node ID:** This field is only shown when PRTG is running in a cluster mode. This setting is shown for your information only and cannot be changed here.

Cluster Mode Actions Depending on the current cluster settings, you see different active buttons here.

- **Create a PRTG Cluster...**
- **Join a PRTG Cluster...**
- **Change PRTG Cluster Settings...**
- **Revert to Standalone...**

 For details on these options, see [below this table](#) .

Master Heartbeat This section is only visible if you are running your PRTG installation in cluster mode. The **current** master can execute an external executable file on a regular basis. We call this a "heartbeat".

You can use this, for example, to report the IP address of the current master node to a dynamic DNS provider, so a DNS name is always redirected to the current PRTG master node in case the original master node fails and a failover node (running at a different IP address) takes over the master role.

Choose between:

- **No heartbeat:** Do not execute a file on a regular basis.
- **Run the following external executable file every 5 minutes:** Click the ... button to choose a file you want to execute. This can be, for example, a command line tool, or a batch file. It will be executed on the current master node only, with a fixed interval of five minutes. The interval cannot be changed.

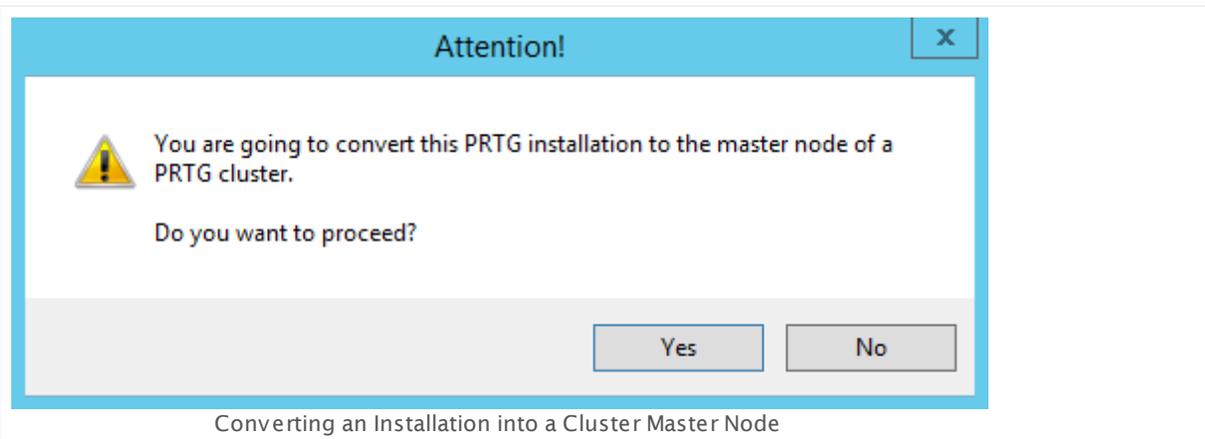
 Please make sure that the selected file is available under the same (local) path on all failover nodes. In case one of your failover nodes becomes current master, the heartbeat can only be executed reliably if the executable file exists on all of your failover nodes.

Cluster Mode Actions

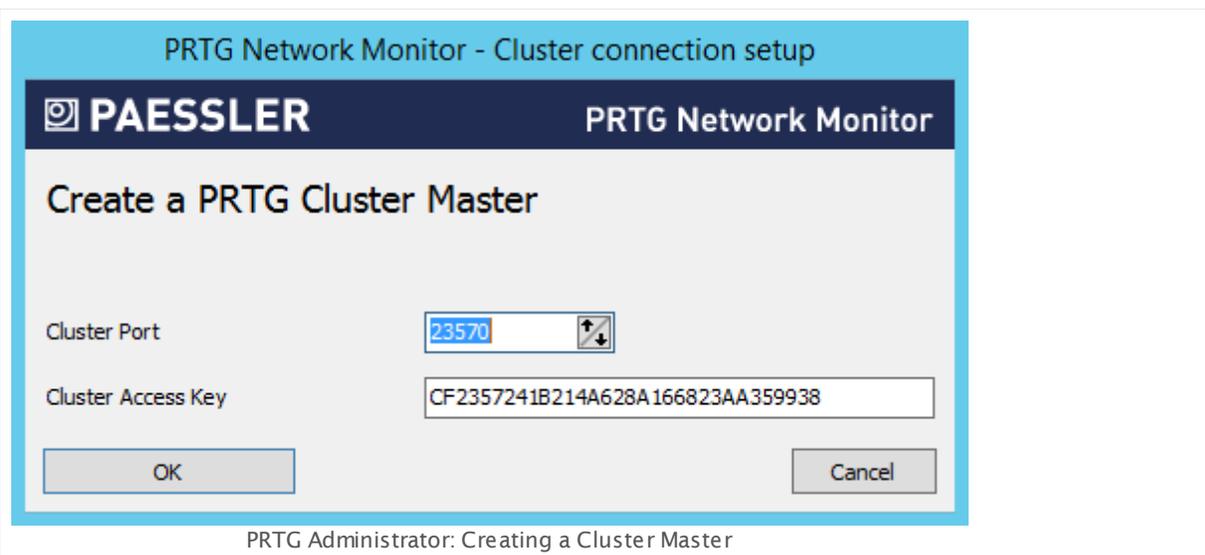
Follow these instructions to create or join a cluster, to change a cluster's settings, or to revert a cluster node to a standalone PRTG installation:

Create a PRTG Cluster...

- Click this button to start creating a cluster. The current PRTG core server will then be the **Master Node** of your cluster.
- Click **Yes** to confirm the conversion of this installation into a cluster master node.



- A new dialog box will appear.

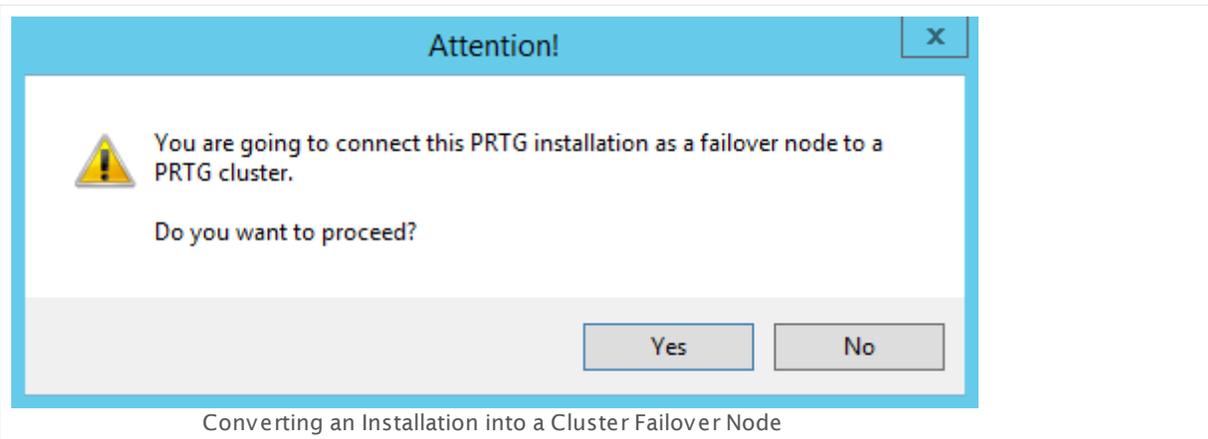


- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend that you use the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your **Failover Node(s)**.

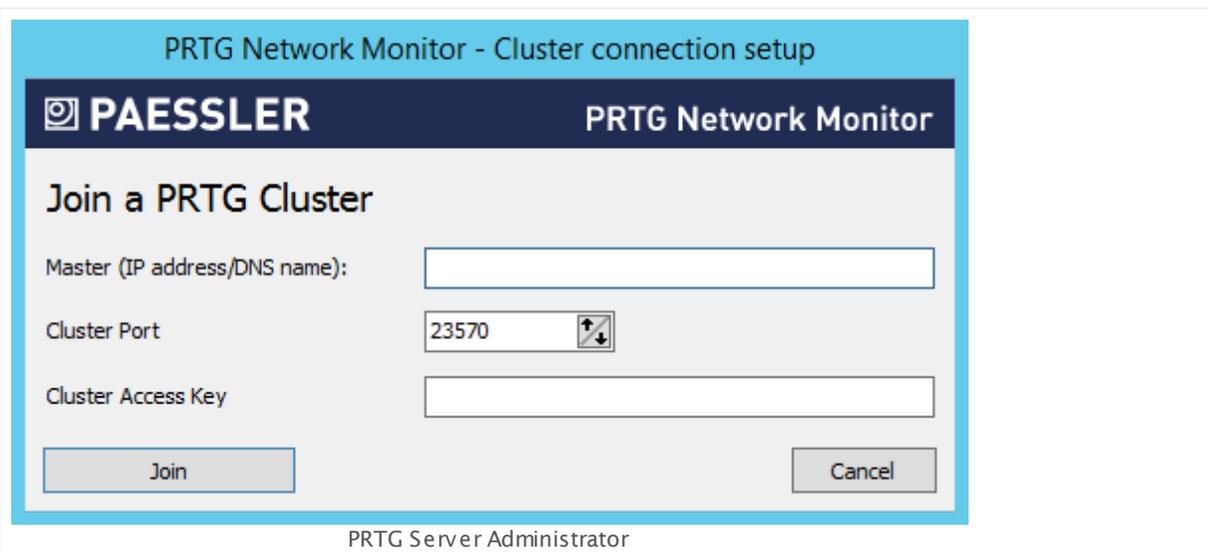
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Join a PRTG Cluster...

- Click this button to add this installation to an existing cluster that already has a **Master Node**. The current PRTG core server will then be a **Failover Node** in the cluster.
- This button is also available if you are currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- Click **Yes** to confirm the conversion of this installation into a failover node.



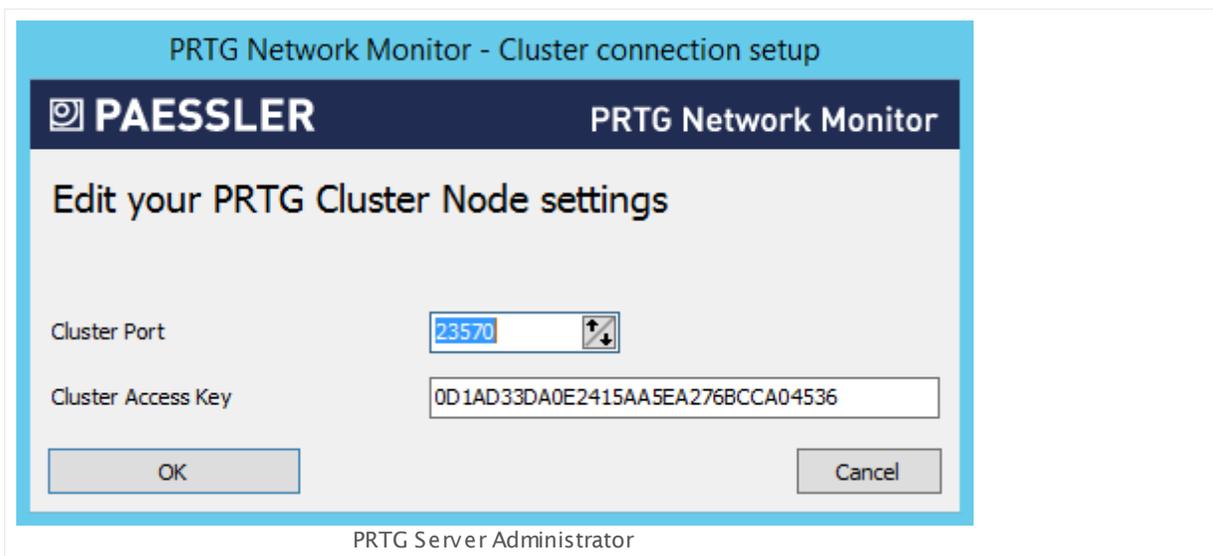
- A dialog box will appear.



- Enter a **Master IP address/DNS name** for your cluster. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in the settings of your **Master Node**. Please make sure you use the same settings on all nodes in your cluster.

- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Change PRTG Cluster Settings...



- If you are running your PRTG installation in cluster mode, you can change the settings here. A new window will appear.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- Please make sure you use the same settings on all nodes in your cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

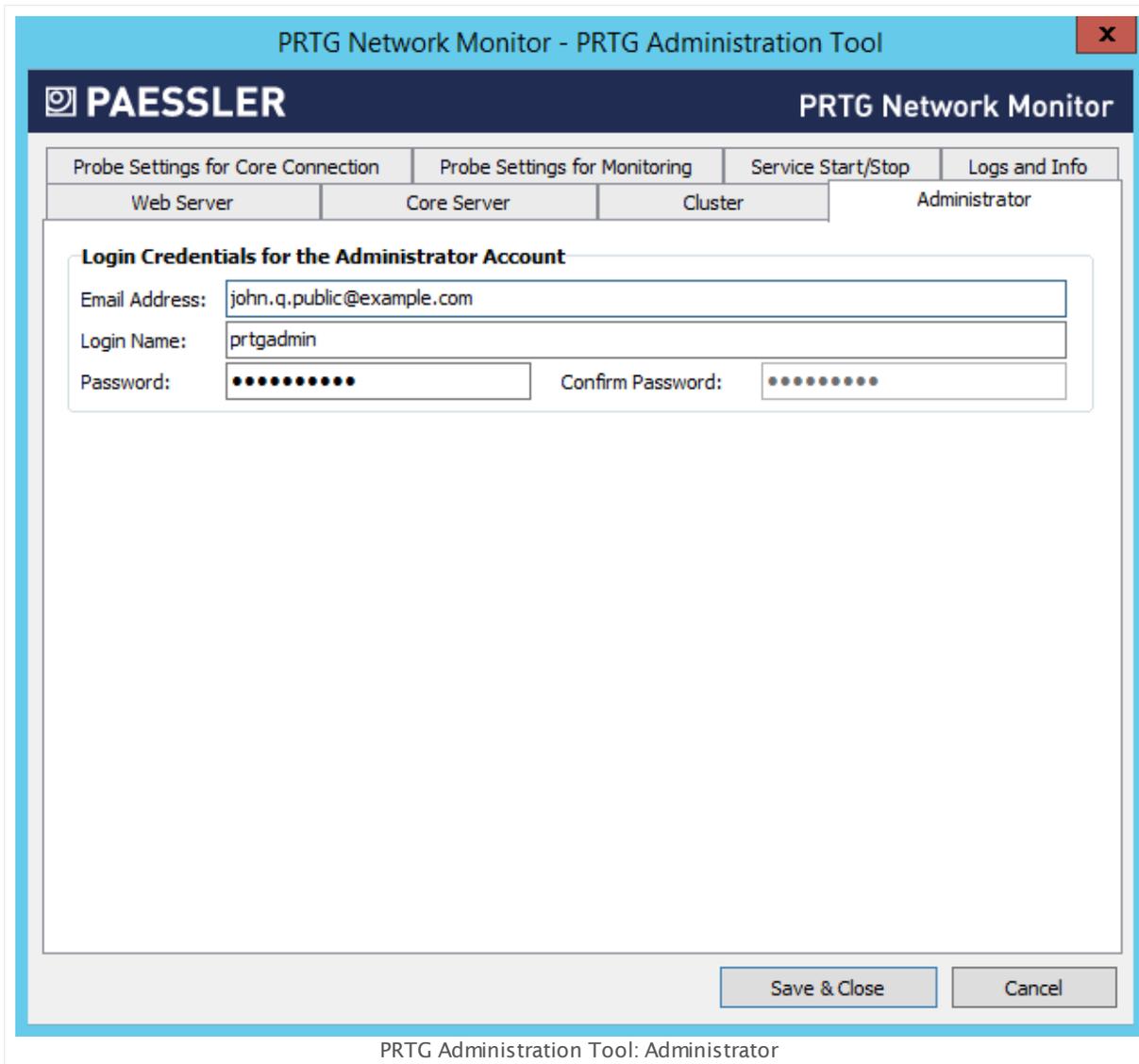
Revert to Standalone...

- If you are currently running your PRTG installation in cluster mode, you can change it to **Standalone** mode. If you do so, this node will no longer be part of a cluster.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Administrator

Change PRTG System Administrator specific settings.

- i** You can also change these settings in the [account settings](#)³⁵⁷⁷ of the **PRTG System Administrator** user in the PRTG web interface.



The screenshot shows the 'Administrator' tab within the 'PRTG Administration Tool' window. The window title is 'PRTG Network Monitor - PRTG Administration Tool'. The interface includes the PAESSLER logo and 'PRTG Network Monitor' text. A navigation bar contains tabs for 'Probe Settings for Core Connection', 'Probe Settings for Monitoring', 'Service Start/Stop', and 'Logs and Info'. Below this, there are sub-tabs for 'Web Server', 'Core Server', 'Cluster', and 'Administrator'. The 'Administrator' tab is active, displaying a section titled 'Login Credentials for the Administrator Account'. This section contains four input fields: 'Email Address' (with the value 'john.q.public@example.com'), 'Login Name' (with the value 'prtgadmin'), 'Password' (masked with dots), and 'Confirm Password' (also masked with dots). At the bottom right of the form are 'Save & Close' and 'Cancel' buttons. The caption below the screenshot reads 'PRTG Administration Tool: Administrator'.

LOGIN CREDENTIALS FOR THE ADMINISTRATOR ACCOUNT

Email Address

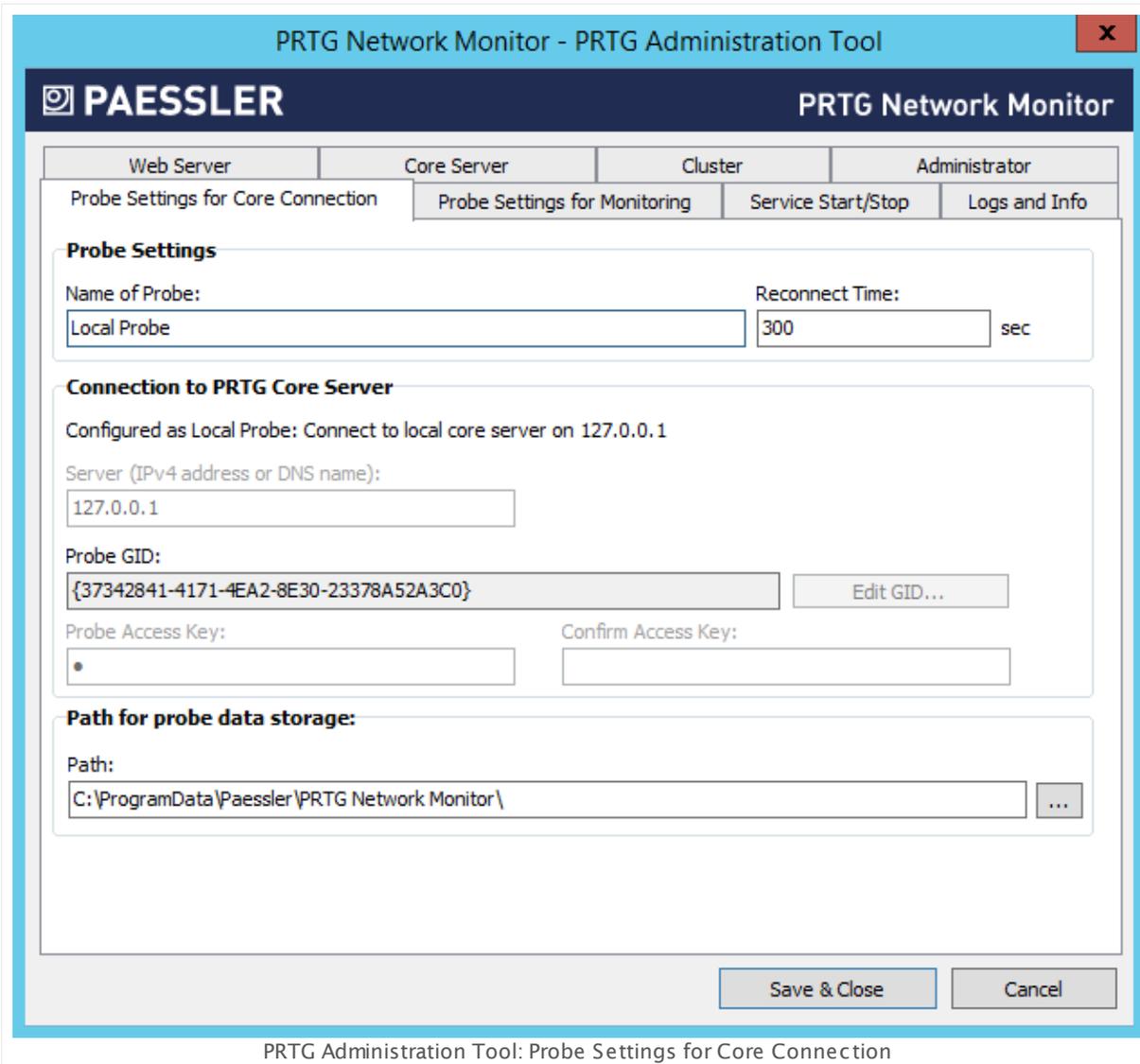
Enter a valid email address for the administrator. By default, PRTG will send notifications and important messages to this address.

LOGIN CREDENTIALS FOR THE ADMINISTRATOR ACCOUNT

Login Name	<p>Enter a name for the PRTG System Administrator login. This is your default login! You use it when you log in to the PRTG web interface or Enterprise Console.</p> <p> The default login name is prtadmin.</p>
Password	<p>Enter a password for the PRTG System Administrator login. This is your default login! You use it when you log in to the PRTG web interface or Enterprise Console.</p> <p> The default password is prtadmin.</p>
Confirm Password	<p>If you change your password, re-enter the password for the PRTG System Administrator login to confirm it.</p>

Probe Settings for Core Connection

Define general settings regarding the probe and probe connections.



PRTG Administration Tool: Probe Settings for Core Connection

PROBE SETTINGS

- Name of Probe** Enter a meaningful name to identify the probe. PRTG shows this name, for example, in the device tree, and in all alarms by default. Please enter a string.
- Reconnect Time** Define the time that PRTG will wait until the probe tries to reconnect to the core server if the connection fails. Please enter an integer value.

CONNECTION TO PRTG CORE SERVER

These settings affect the way the probe will connect to the core server. A probe is either a local probe, a hosted probe, or a remote probe. PRTG will automatically detect the type of probe and show the correct setting options.

Server (IPv4 address or DNS name)	<p>If this probe is configured as the Local Probe of the PRTG core installation, it will connect to the core via 127.0.0.1, which you cannot change.</p> <p>If this probe is configured as a Remote Probe, enter the IP address or DNS name of the core server.</p>
Probe GID	<p>The Probe GID (global ID (GID)) is a unique identifier for the probe. We recommend that you do not change it.</p> <p>Exception: Only if you substitute an existing remote probe from a different computer, you have to copy the GID from the old probe to the new probe. To do so, click the Edit GID... button and confirm the warning with Yes. You can then change the value. You cannot change the GID for a local probe.</p> <p>i You can deny GIDs under System Administration—Core & Probes in the PRTG web interface. If you remove a remote probe from the device tree or if you deny a remote probe after installation, its global ID (GID) will be automatically entered in the Deny GIDs list.</p>
Probe Access Key	<p>You do not need an access key for Local Probe connections.</p> <p>On a Remote Probe, the Probe Access Key must match one of the access keys configured in your PRTG core server installation. If it does not match, the remote probe will not be able to connect to the core server. See the System Administration—Core & Probes section for more information.</p> <p>i Check also allowed and denied IPs in System Administration—Core & Probes to ensure that the core server accepts the IP address of the remote probe.</p>
Confirm Access Key	<p>If you enter an access key for a remote probe, enter it in this field again to assure correctness.</p>

PATH FOR PROBE DATA STORAGE

Path	<p>Define the data folder to which PRTG will store configuration and monitoring data. Click the ... button to choose another folder on your system.</p>
------	---

PATH FOR PROBE DATA STORAGE

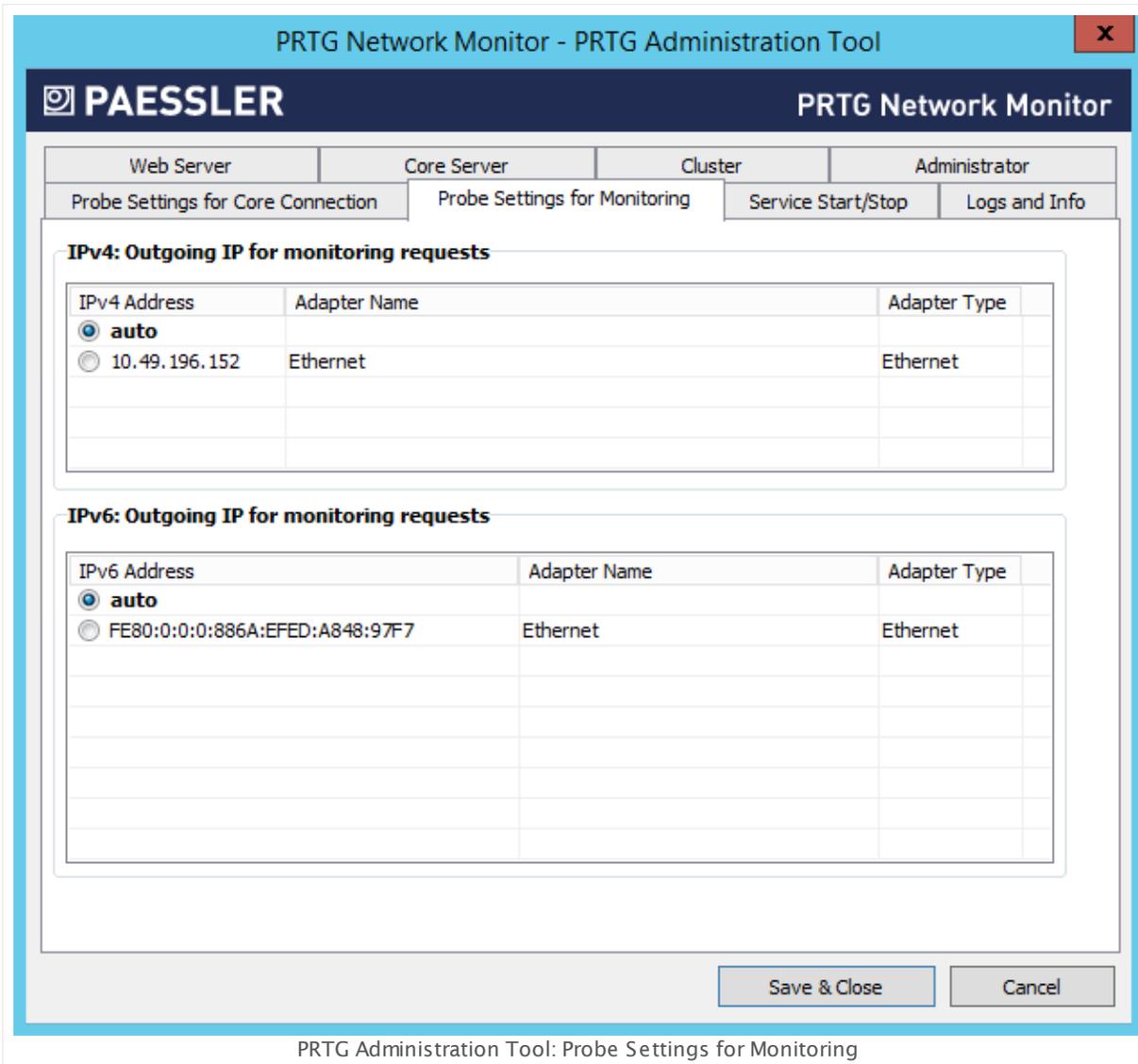
 Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location.

LANGUAGE FOR THE PRTG ADMINISTRATION TOOL FOR REMOTE PROBES

<your language>

Choose the language for the PRTG Administration Tool on your remote probe from the dropdown list. Default is **English**.

Probe Settings for Monitoring



PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.

PROBE SETTINGS FOR MONITORING

- The setting is valid for all monitoring requests sent from this PRTG probe.
- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

 This feature does not support all sensor types for technical reasons.

 If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

Outgoing IPv4 Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

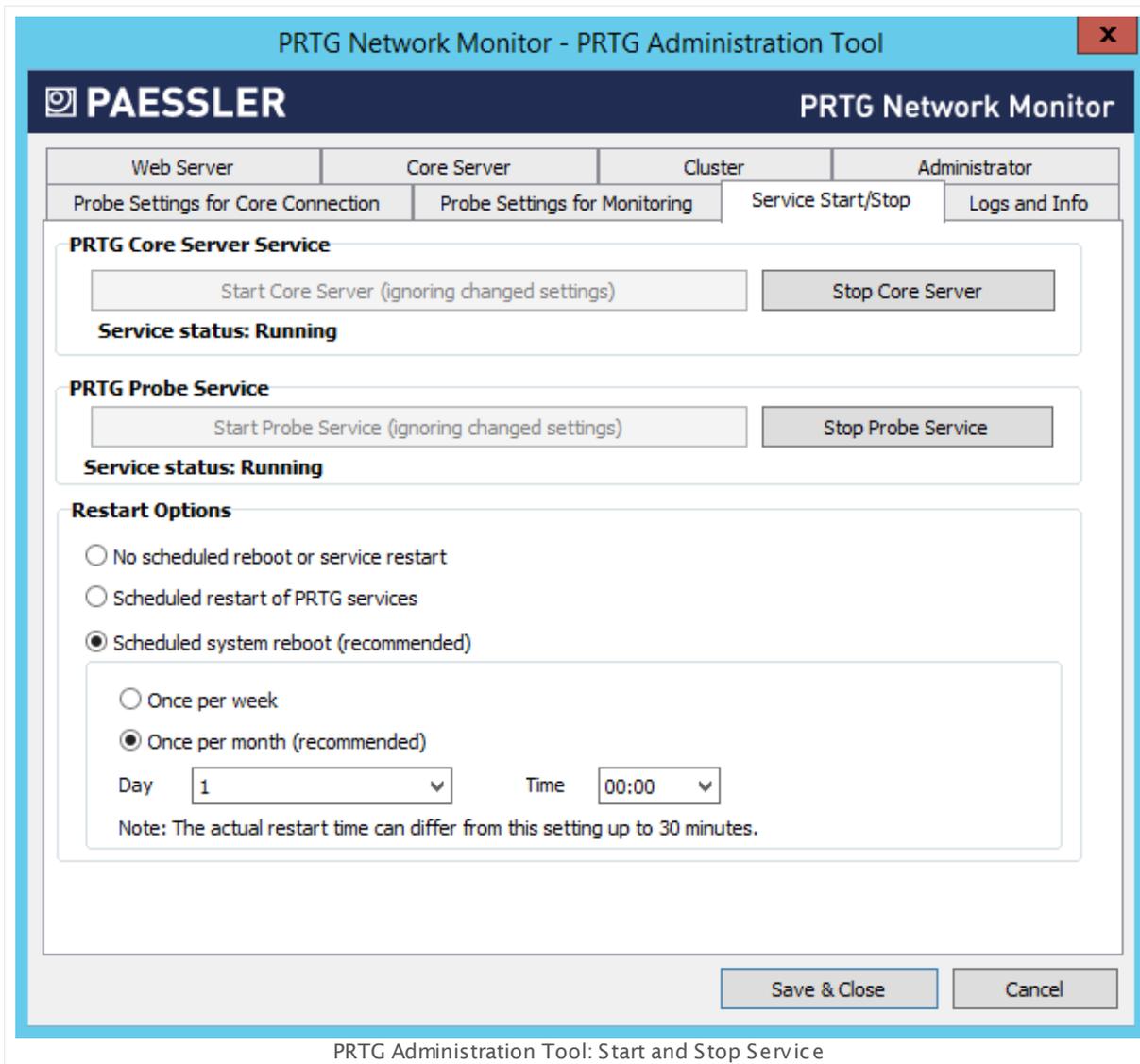
Outgoing IPv6 Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

 For details about the basic concept of IPv6 in PRTG, see the [IPv6](#) ¹⁶³ section.

Service Start/Stop

You can stop and start PRTG Windows services manually. For connected probes, click **Start Core Server** to start the service or **Stop Core Server** to stop it. Both actions usually take from a few seconds up to several minutes to complete. You can also restart the core server and connected probes via the PRTG web interface under [Administrative Tools](#) ³³⁸⁸.

 We recommend that you set a schedule for automatic system restarts.



You can also define a restart schedule on the [Settings](#)³⁵¹ tab of a probe under **Restart Options**, in the PRTG web interface.

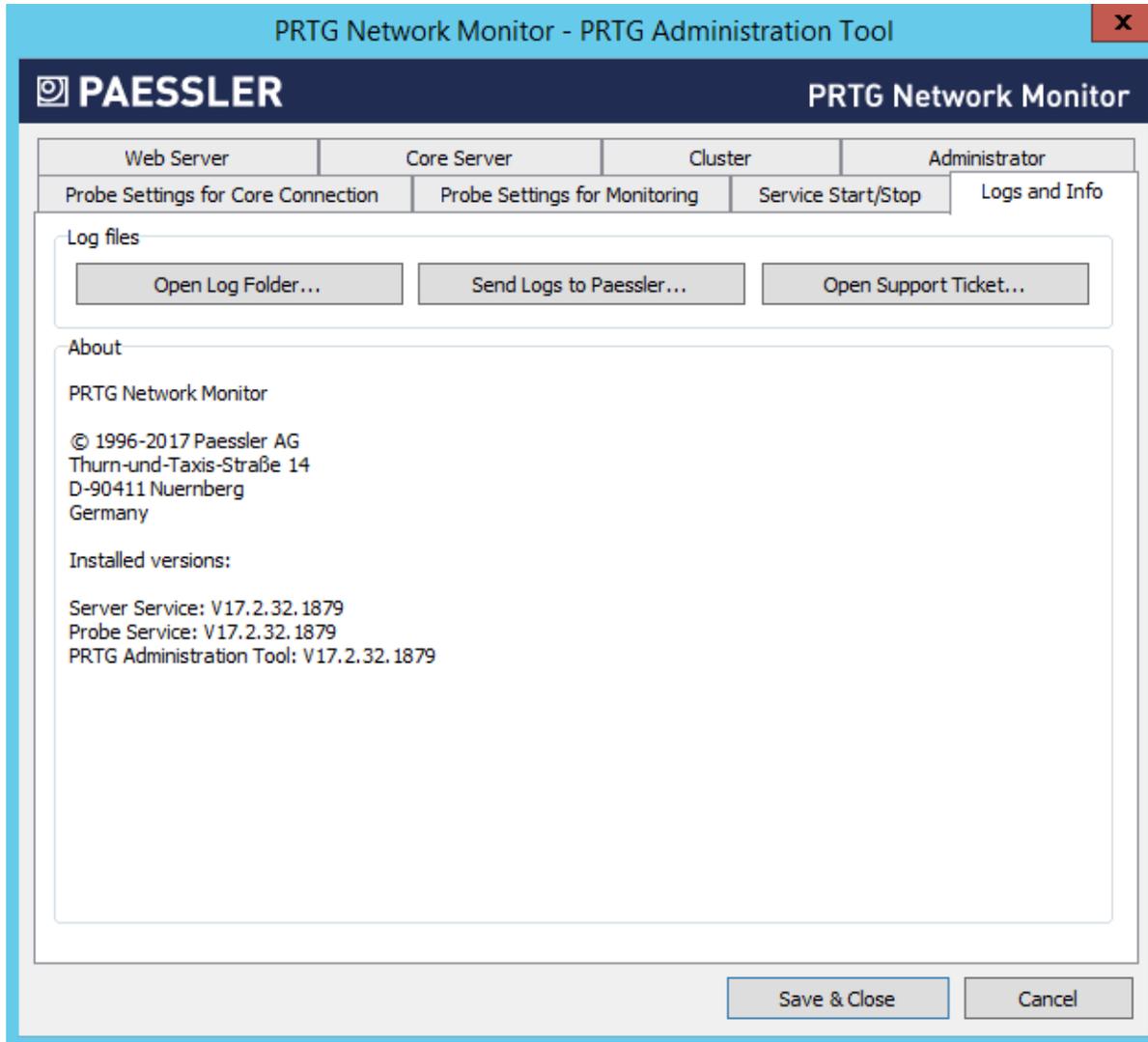
SCHEDULED RESTART SETTINGS

 This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SCHEDULED RESTART SETTINGS

Restart Options	<p>For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options:</p> <ul style="list-style-type: none">▪ No scheduled reboot or service restart: Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under System Administration—Administrative Tools <small>3388</small> in the PRTG web interface.▪ Scheduled restart of PRTG services: Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below.▪ Scheduled system reboot (recommended): We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.
Restart Schedule	<p>You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server:</p> <ul style="list-style-type: none">▪ Once per week: Select a day of the week and a time below.▪ Once per month (recommended): Select a day of the month and a time below.
Specify Day	<p>You can only see this setting if you selected a schedule option above. Select a specific day of the week (Monday to Sunday) or month (1st to 30th or Last). If you select Last, the restart will always be executed on the last day of the month, regardless of how many days the month has.</p> <p>i If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.</p>
Specify Hour	<p>You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart.</p> <p>i You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.</p>

Logs and Info



PRTG Administration Tool: Logs and Info

LOG FILES

Open Log Folder...

Open the PRTG Network Monitor data directory on your hard disk drive to access all logfiles that PRTG creates.

Send Logs to Paessler...

Open an assistant to send logfiles to the Paessler Support Team. See [below for details](#).



You can send logfiles more easily with the support bundle via [Contact Support](#) in the PRTG web interface.

LOG FILES

Open Support Ticket... This will open the support form on the Paessler website in a browser window.

 If you need help, we recommend that you use the [Contact Support](#)  option in the PRTG web interface instead.

The **About** section shows information about the version of installed PRTG programs and copyright.

Send Logs to Paessler

 You can send logfiles more easily with the support bundle via [Contact Support](#)  in the PRTG web interface.

Send Logs to Paessler

PAESSLER
PRTG Network Monitor

Send Logs to Paessler

Name

Email

Ticket No.

Please supply your Paessler Ticket Number (PAEXXXX) if you already have an open support ticket.

Configuration Include Configuration file (contains passwords)

Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.

If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Please note: Support communication can be provided in English or German only!

Send Logs to Paessler

If you open a support ticket, Paessler Support might ask you to send logfiles for further analysis. With the **Send Logs to Paessler...** button, PRTG will automatically collect, compress, and send your logfiles to our FTPS server.

SEND LOGS TO PAESSLER

Name

SEND LOGS TO PAESSLER

Email	Enter a valid email address. You can provide any of your addresses, but we recommend that you use the email address of your PRTG account, which is entered by default.
Ticket No.	<p>This field is optional. If you have already opened a ticket at Paessler Support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.</p> <p>Please enter the ticket number starting with PAE followed by four or more digits, for example, PAE12345. If you do not have a ticket number, leave this field empty.</p>
Configuration	Define if you want to include the configuration file in the data. PRTG will remove all passwords from the config file before sending it to our support team.

Click the **Send** button to start the data upload. Ensure that FTPS and HTTP connections are allowed on this machine.

More

Video Tutorial: The PRTG Administration Tool

- <https://www.paessler.com/support/videos/prtg-basics/administration-tool>

Knowledge Base: Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>

12.2 PRTG Administration Tool on Remote Probe Systems

If you start the **PRTG Administration Tool** on a system on which a PRTG [Remote Probe](#)^[3709] runs, you can define various probe related settings, restart services, and view log information. You can also change many of these settings via the [system administration](#)^[3302] and the [probe settings tab](#)^[371] in the [PRTG web interface](#)^[166].

-  This section describes the available settings in the PRTG Administration Tool when you open the tool on a **PRTG remote probe system**. This is not the complete set of available settings. If you need access to all possible settings regarding your whole PRTG installation, open the PRTG Administration Tool on the PRTG core server machine.
-  All settings you make here are valid only for the local installation running on the computer on which you open the PRTG Administration Tool. In order to change settings for another installation, for example, another remote probe installation, please log in to that computer and open the program there.
-  To get familiar with the different components of PRTG, we recommend that you read the [Architecture](#)^[125] section. If you prefer a video introduction to the **PRTG Administration Tool**, see the [More](#)^[3586] section below for more information.

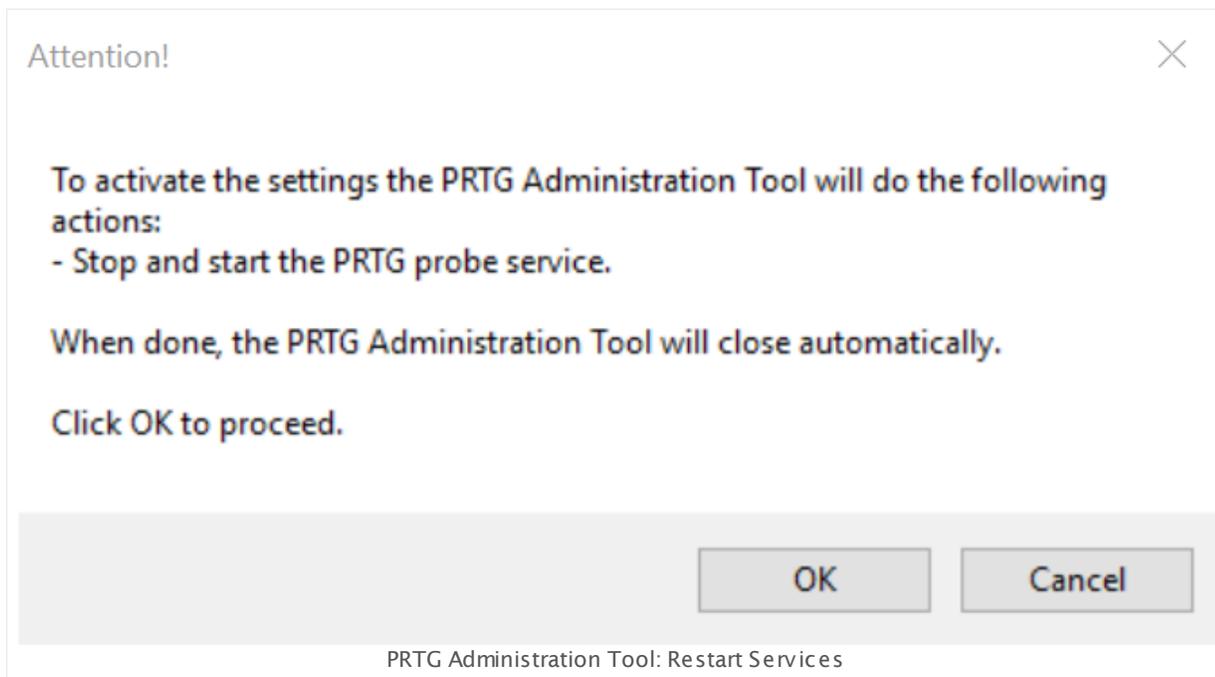
Start the PRTG Administration Tool

From the Windows start menu, select the **PRTG Network Monitor** group and click **PRTG Administration Tool** to open the application.

You can choose from these options in different tabs:

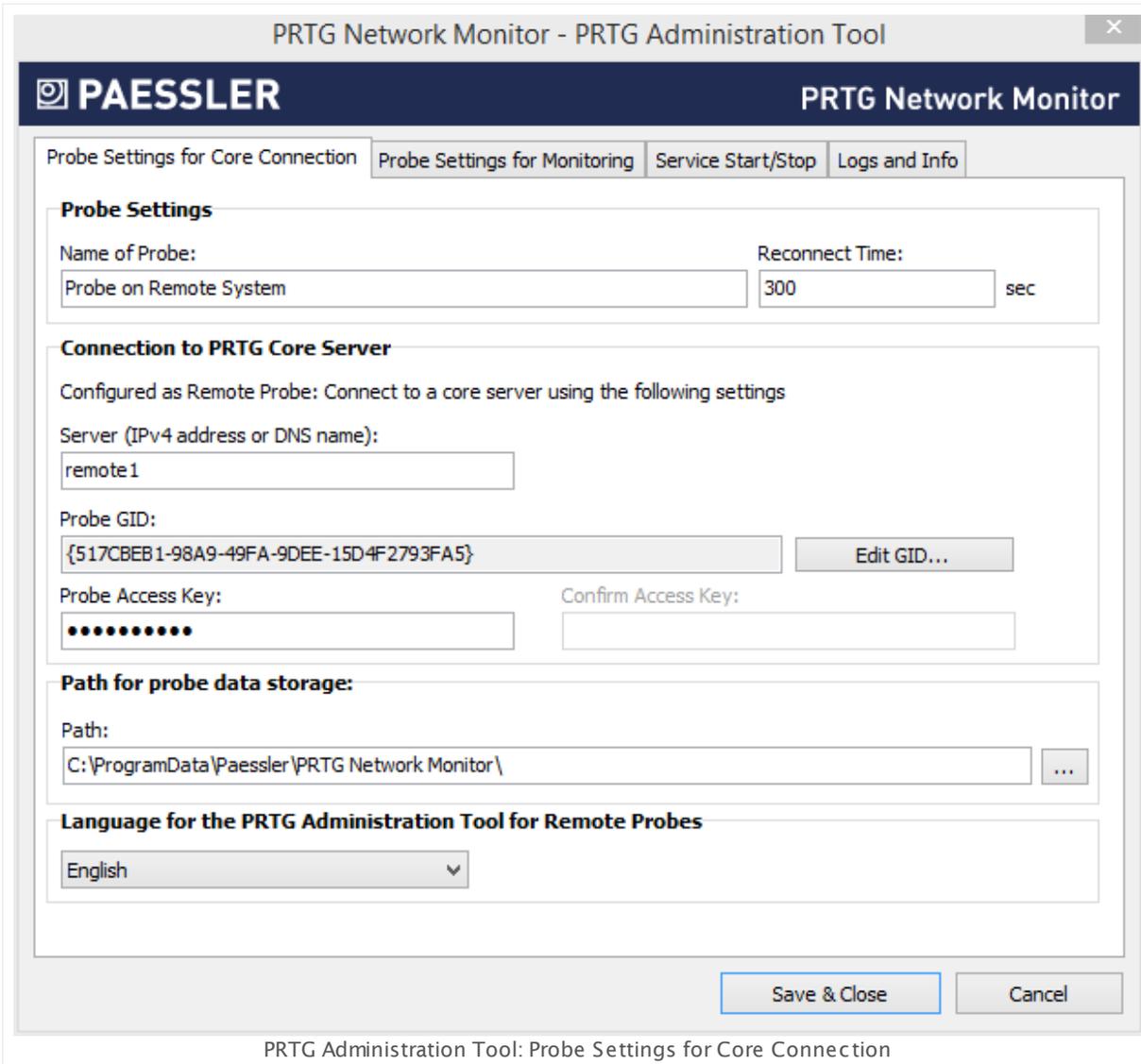
- [Probe Settings for Core Connection](#)^[3588]
- [Probe Settings for Monitoring](#)^[3592]
- [Service Start/Stop](#)^[3593]
- [Logs and Info](#)^[3596]

After you have changed settings, click the **Save & Close** button. A new window opens where PRTG asks you to agree to restart the PRTG core server service. Click **OK** if you do not want your changes to be ignored.



Probe Settings for Core Connection

Define general settings regarding the probe and probe connections.



PROBE SETTINGS

- Name of Probe Enter a meaningful name to identify the probe. PRTG shows this name, for example, in the device tree, and in all alarms by default. Please enter a string.

- Reconnect Time Define the time that PRTG will wait until the probe tries to reconnect to the core server if the connection fails. Please enter an integer value.

CONNECTION TO PRTG CORE SERVER

These settings affect the way the probe will connect to the core server. A probe is either a local probe, hosted probe, or a remote probe. PRTG will automatically detect the type of probe and show the correct setting options.

Server (IPv4 address or DNS name)	<p>If this probe is configured as the Local Probe of the PRTG core installation, it will connect to the core via 127.0.0.1, which you cannot change.</p> <p>If this probe is configured as a Remote Probe, enter the IP address or DNS name of the core server.</p>
Probe GID	<p>The Probe GID (global ID (GID)) is a unique identifier for the probe. We recommend that you do not change it.</p> <p>Exception: Only if you substitute an existing remote probe from a different computer, you have to copy the GID from the old probe to the new probe. To do so, click on the Edit GID... button and confirm the warning with Yes. You can then change the value. You cannot change the GID for a local probe.</p> <p>i You can deny GIDs under System Administration—Core & Probes^[3369] in the PRTG web interface. If you remove a remote probe from the device tree or if you deny a remote probe after installation^[107], its global ID (GID) will be automatically entered in the Deny GIDs list.</p>
Probe Access Key	<p>You do not need an access key for Local Probe connections.</p> <p>On a Remote Probe, the Probe Access Key must match one of the access keys configured in your PRTG core server installation. If it does not match, the remote probe will not be able to connect to the core server. See the System Administration—Core & Probes^[3369] section for more information.</p> <p>i Check also allowed and denied IPs in System Administration—Core & Probes^[3369] to ensure that the core server accepts the IP address of the remote probe.</p>
Confirm Access Key	<p>If you enter an access key for a remote probe, enter it in this field again to assure correctness.</p>

PATH FOR PROBE DATA STORAGE

Path	<p>Define the data folder to which PRTG will store configuration and monitoring data. Click the ... button to choose another folder on your system.</p>
------	---

PATH FOR PROBE DATA STORAGE

 Before you change the path, make sure you stop both the core server and the probe services and copy all data to the new location.

LANGUAGE FOR THE PRTG ADMINISTRATION TOOL FOR REMOTE PROBES

<your language>

Choose the language for the PRTG Administration Tool on your remote probe from the dropdown list. Default is **English**.

Probe Settings for Monitoring

PRTG Network Monitor - PRTG Administration Tool

PAESSLER PRTG Network Monitor

Probe Settings for Core Connection | **Probe Settings for Monitoring** | Service Start/Stop | Logs and Info

IPv4: Outgoing IP for monitoring requests

IPv4 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> 192.168.1.1	Ethernet 2	Ethernet
<input type="radio"/> 192.168.1.100	Wi-Fi	IEEE80211

IPv6: Outgoing IP for monitoring requests

IPv6 Address	Adapter Name	Adapter Type
<input checked="" type="radio"/> auto		
<input type="radio"/> FD32:5A88:8E98:2:0:0:0:1001	Ethernet 2	Ethernet
<input type="radio"/> FE80:0:0:0:3873:CCBA:9FA6:42C4	Ethernet 2	Ethernet
<input type="radio"/> 2003:71:8F3B:CC7B:551F:4D00:54AB:AA0F	Wi-Fi	IEEE80211
<input type="radio"/> 2003:71:8F3B:CC7B:1CCF:C12:7BF3:236	Wi-Fi	IEEE80211
<input type="radio"/> FE80:0:0:0:551F:4D00:54AB:AA0F	Wi-Fi	IEEE80211
<input type="radio"/> FD13:721E:D424:1000:E4F6:5BEE:188:3992	iphhttpsinterface	Tunnel
<input type="radio"/> FD13:721E:D424:1000:841F:6929:FB37:C191	inhhttpsinterface	Tunnel

Save & Close Cancel

PRTG Administration Tool: Probe Settings for Monitoring

PROBE SETTINGS FOR MONITORING

Define the IP address used for outgoing monitoring requests.

- If there is more than one IP on the current system available, you can specify the IP address that PRTG will use for outgoing monitoring requests of certain sensor types.
- This setting will be used for sensors using the following connection types: HTTP, DNS, FTP, IMAP, POP3, Port, Remote Desktop, SMTP, and SNMP.
- The setting is valid for all monitoring requests sent from this PRTG probe.

PROBE SETTINGS FOR MONITORING

- This setting is useful for devices that expect a certain IP address when queried.
- Default setting is **auto**. PRTG will select an IP address automatically.

 This feature does not support all sensor types for technical reasons.

 If you change this setting, some sensors might stop working. For example, sensors might show a **Down** status if the selected IP address is blocked on the way to or directly on the monitored device.

Outgoing IPv4 Define the IP address for outgoing requests using the IPv4 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

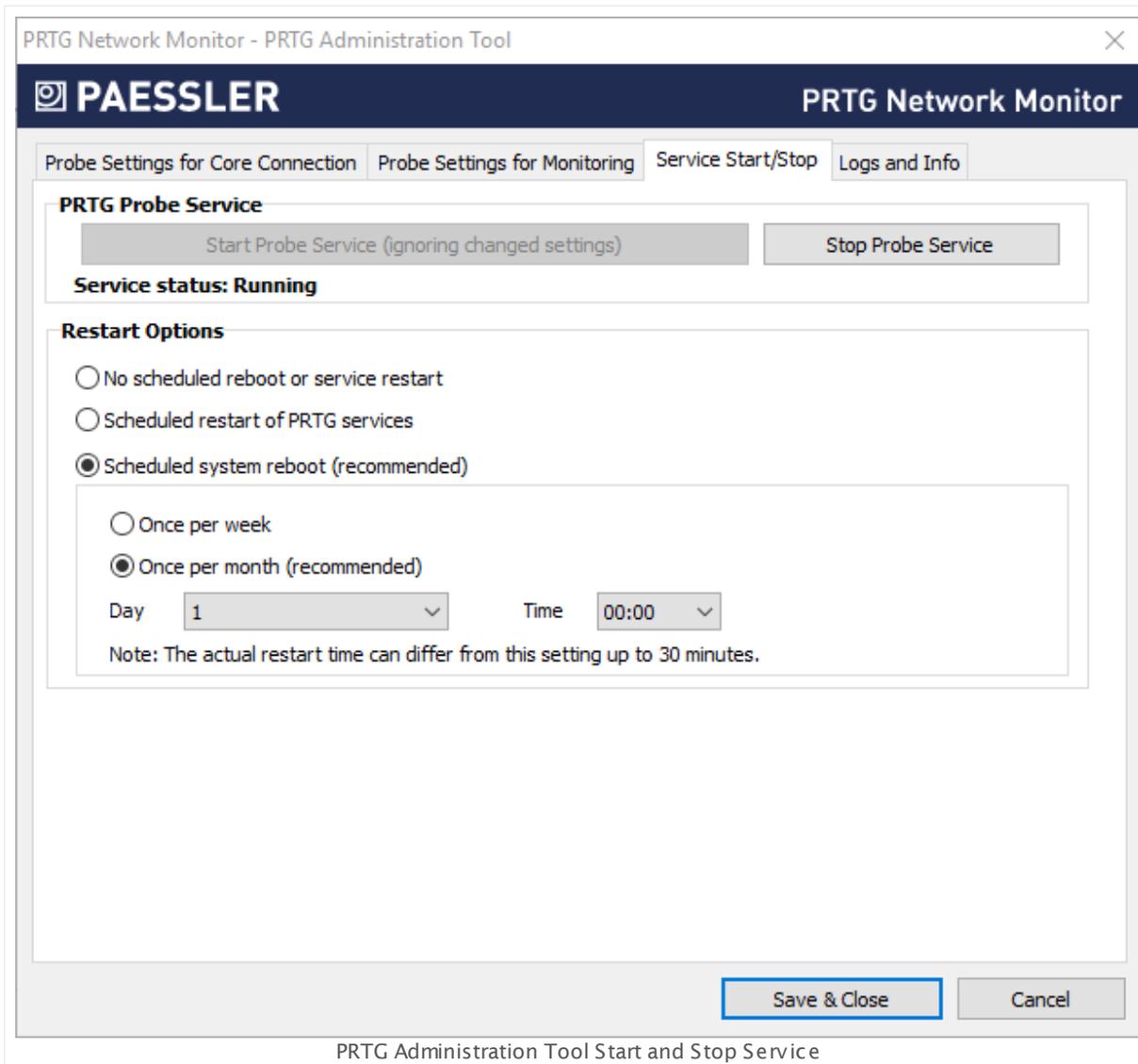
Outgoing IPv6 Define the IP address for outgoing requests using the IPv6 protocol. The list shows all IP addresses available on the current system. Choose a specific IP address or select **auto**.

 For details about the basic concept of IPv6 in PRTG, see the [IPv6](#) section.

Service Start/Stop

You can stop and start PRTG Windows services manually. For connected probes, click **Start Probe Service** to start the service or **Stop Probe Service** to stop it. Both actions usually take from a few seconds up to several minutes to complete. You can also restart the core server and connected probes via the PRTG web interface under [Administrative Tools](#).

 We recommend that you set a schedule for automatic restarts.



You can also define a restart schedule on the [Settings](#)^[35] tab of a probe under **Restart Options**, in the PRTG web interface.

SCHEDULED RESTART SETTINGS

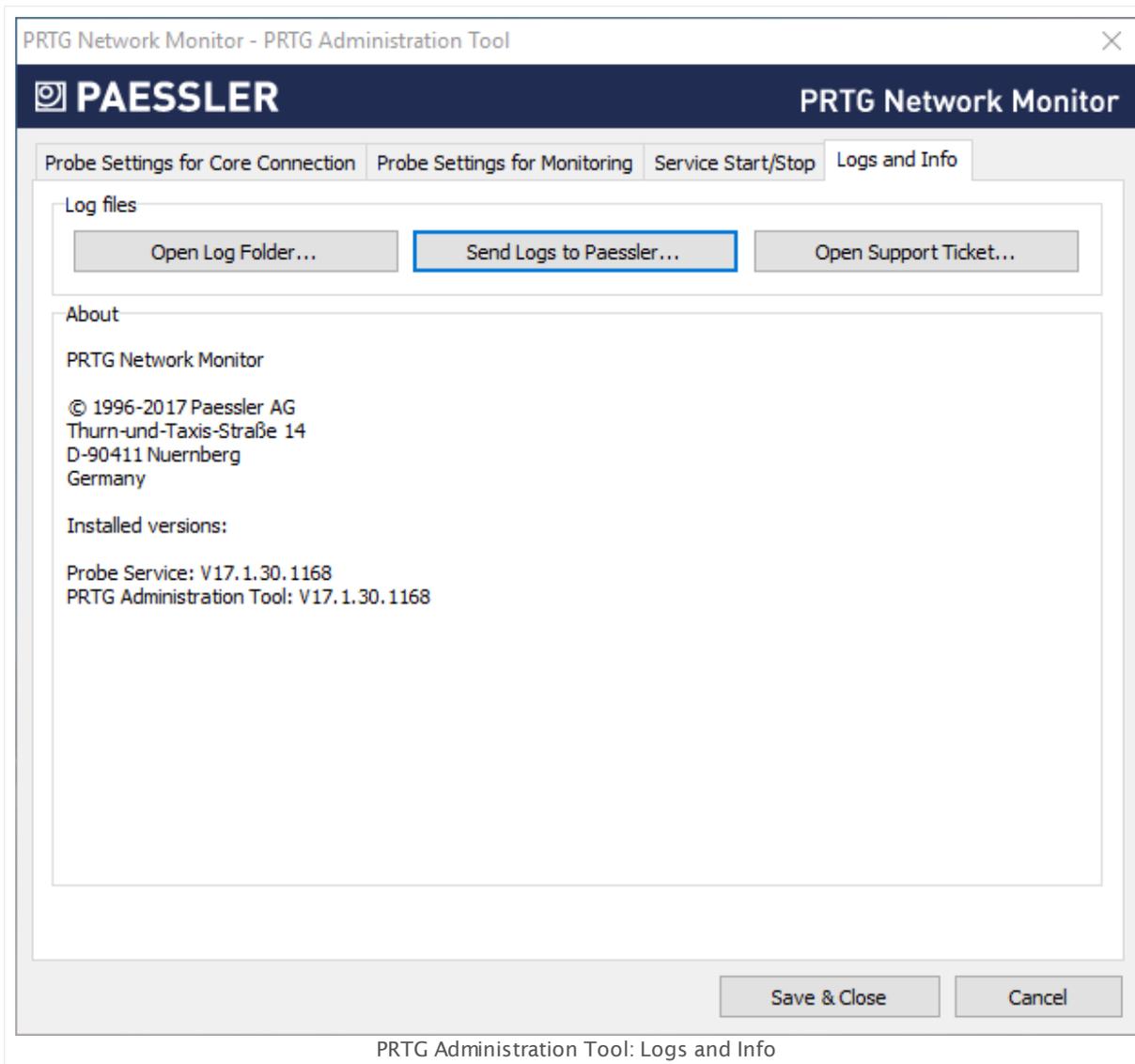
 This setting is not available on the **Hosted Probe** of a PRTG hosted by Paessler instance.

SCHEDULED RESTART SETTINGS

Restart Options	<p>For best performance, we recommend that you regularly restart the Windows servers on which PRTG is running. To do this automatically for PRTG, you can schedule an automatic restart. Choose between the following options:</p> <ul style="list-style-type: none">▪ No scheduled reboot or service restart: Do not perform any scheduled restart of services automatically. We recommend a manual restart every few weeks. You can initiate a restart of your PRTG core server and probes under System Administration—Administrative Tools³³⁸⁸ in the PRTG web interface.▪ Scheduled restart of PRTG services: Restart all PRTG services on the system where this probe runs on. If you choose this option on the local probe, the PRTG core server will restart as well. Define a schedule below.▪ Scheduled system reboot (recommended): We recommend this setting, although it is not set by default. Enter a schedule below. We recommend that you restart Windows servers once a month for best performance.
Restart Schedule	<p>You can only see this setting if you selected a schedule option above. Choose how often you want to restart PRTG services or the Windows server:</p> <ul style="list-style-type: none">▪ Once per week: Select a day of the week and a time below.▪ Once per month (recommended): Select a day of the month and a time below.
Specify Day	<p>You can only see this setting if you selected a schedule option above. Select a specific day of the week (Monday to Sunday) or month (1st to 30th or Last). If you select Last, the restart will always be executed on the last day of the month, regardless of how many days the month has.</p> <p>i If you select a date that does not exist in every month (for example, the 30th day in February), PRTG will automatically initiate the restart on the last day of this month.</p>
Specify Hour	<p>You can only see this setting if you selected a schedule option above. Select the time of day when PRTG will perform the restart.</p> <p>i You will get a Windows warning message 10 minutes before the restart to inform you if you are a currently logged in user. The actual restart time can differ up to 30 minutes from the settings you enter here.</p>

i You can also define a restart schedule on the **Settings** tab of a probe, section [Scheduled Restart Settings](#)³⁷¹, in the PRTG web interface.

Logs and Info



LOG FILES

Open Log Folder...

Open the PRTG Network Monitor data directory on your hard disk drive to access all logfiles that PRTG creates.

Send Logs to Paessler...

Open an assistant to send logfiles to the Paessler Support Team. See [below for details](#).

i You can send logfiles more easily with the support bundle via [Contact Support](#) in the PRTG web interface.

LOG FILES

Open Support Ticket... This will open the support form on the Paessler website in a browser window.

 If you need help, we recommend that you use the [Contact Support](#)³⁴²⁷ option in the PRTG web interface instead.

The **About** section shows information about the version of installed PRTG programs and copyright.

Send Logs to Paessler

 You can send logfiles more easily with the support bundle via [Contact Support](#)³⁴²⁷ in the PRTG web interface.

Send Logs to Paessler

PAESSLER
PRTG Network Monitor

Send Logs to Paessler

Name

Email

Ticket No.

Please supply your Paessler Ticket Number (PAEXXXX) if you already have an open support ticket.

Configuration Include Configuration file (contains passwords)

Note: while passwords are usually encrypted the configuration file contains SNMP communities and hostnames in plain text.

If you click the "Send" button, this program will upload the relevant log files and, if selected, the configuration file of your PRTG installation to Paessler's FTP server and support ticketing system.

Please ensure that outgoing FTP and HTTP connections are enabled on this machine.

Please note: Support communication can be provided in English or German only!

Send Logs to Paessler

If you open a support ticket, Paessler Support might ask you to send logfiles for further analysis. With the **Send Logs to Paessler...** button, PRTG will automatically collect, compress, and send your logfiles to our FTPS server.

SEND LOGS TO PAESSLER

Name Enter your name.

Email Enter a valid email address. You can provide any of your addresses, but we recommend that you use the email address of your PRTG account, which is entered by default.

SEND LOGS TO PAESSLER

Ticket No.	<p>This field is optional. If you have already opened a ticket at Paessler Support, please provide the ticket number you received. Your files will then be associated with your ticket automatically.</p> <p>Please enter the ticket number starting with PAE followed by four or more digits, for example, PAE12345. If you do not have a ticket number, leave this field empty.</p>
Configuration	<p>Define if you want to include the configuration file in the data. PRTG will remove all passwords from the config file before sending it to our support team.</p>

Click the **Send** button to start the data upload. Ensure that FTPS and HTTP connections are allowed on this machine.

More

Video Tutorial: The PRTG Administration Tool

- <https://www.paessler.com/support/videos/prtg-basics/administration-tool>

Knowledge Base: Which ports does PRTG use on my system?

- <https://kb.paessler.com/en/topic/61462>

Part 13

Advanced Topics

13 Advanced Topics

In this section, we cover topics that address more advanced PRTG users. If you already have some experience with PRTG, you might want to learn more about the following topics.

Advanced Topics

- [Active Directory Integration](#)  3683
- [Application Programming Interface \(API\) Definition](#)  3686
- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)  3688
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)  3690
- [Define IP Ranges](#)  3692
- [Define Lookups](#)  3693
- [Regular Expressions](#)  3704
- [Add Remote Probe](#)  3707
- [Failover Cluster Configuration](#)  3720
- [Data Storage](#)  3734
- [Using Your Own SSL Certificate](#)  3736
- [Calculating Percentiles](#)  3706

13.1 Active Directory Integration

PRTG offers a detailed rights management via different user groups. For detailed information, see [User Access Rights](#)¹⁵⁸.

To make user management easier, you can integrate an existing Active Directory into PRTG in four steps. During this process, you connect an **Active Directory (AD)** group with a user group in PRTG. All members of your AD group can then log in to PRTG using their AD domain credentials.

 You cannot add single AD users to PRTG, but only allow access for entire groups. PRTG automatically creates a user account for each AD user who logs in to PRTG successfully.

 This feature is not available in PRTG hosted by Paessler.

Step 1: Prepare Your Active Directory

- In your Active Directory, ensure users you want to give access to PRTG are member of the same AD group.
- You can also organize users in different groups, for example, one group whose members will have administrator rights within PRTG, and another one whose members will have read-only rights within PRTG.

Step 2: Prepare Your PRTG Server

- Make sure the computer running PRTG is member of the domain you want to integrate it to. You can check this setting in your machine's **System Properties** (for example, **Control Panel | System and Security | System**, click **Change settings** link).

Step 3: Add Domain and Credentials (optional) to System Settings

- In the PRTG [web interface](#)¹⁶⁶, open the [System Administration—Core & Probes](#)³³⁷² settings.
- In section **Active Directory Integration**, enter the name of your local domain into the **Domain Name** field.
 -  You can only integrate one AD domain into PRTG.
- **Optional:** PRTG uses the same Windows user account that you use to run the **PRTG Core Server Service**. By default, this is the **local system** Windows user account. If this user does not have sufficient rights to query a list of all existing groups from the Active Directory, provide credentials of a user account with full AD access by using the **Use explicit credentials** option as **Access Type**.
 -  If you cannot save changes to **Core & Probes** settings because you get an **Error (Bad Request)** with the message **Active Directory Domain not accessible**, change from "local user" to **Use explicit credentials** for **Active Directory Integration** and provide the correct credentials for your domain.
- **Save** your settings.

Step 4: Add a New User Group

- Switch to the **User Groups** tab (see [System Administration—User Groups](#)^[338]).
- Hover over  and click **Add User Group** to add a new PRTG user group.
- In the dialog appearing, enter a meaningful name and set the **Use Active Directory** setting to **Yes**.
- From the **Active Directory Group** dropdown menu, select the group of your Active Directory whose members will have access to PRTG. If you have a very large Active Directory, you will see an input field instead of a dropdown. In this case, you can enter the group name only; PRTG will add the prefix automatically.
- With the **New User Type** setting, define the [access rights](#)^[158] a user from the selected Active Directory group will have when logging in to PRTG for the first time. You can choose between **Read/Write User** or **Read Only User** (latter is useful to show data only to a large group of users).
- **Save** your settings.

Done

That's it. All users in this Active Directory group can now log in to PRTG using their AD domain credentials. Their user accounts will use the PRTG security context of the PRTG user group you just created.

Notes and Limitations

- Active Directory users can [log on to the web interface](#)^[168] using their Windows username and password (please do not enter any domain information in PRTG's **Login Name** field). When such a user logs in, PRTG will automatically create a corresponding local account on the PRTG core server. Credentials are synchronized every hour.
- All requests to the Active Directory servers are cached for one hour, for performance reasons. If a password is changed in the Active Directory, you must either wait for 1 hour or clear the cache manually by clicking on the **Clear Caches** button on the [System Administration—Administrative Tools](#)^[338] page in the [Setup](#)^[3302] menu).
- By default, there are not set any rights for the new PRTG user group. Initially, users in this group will not see any objects in the PRTG device tree. Edit your device tree [object's settings](#)^[217] and set access rights for your newly created user group in the **Inherit Access Rights** section.
 - ❗ The easiest way is to set access rights in the [Root Group Settings](#)^[331].
- PRTG only supports explicit group rights. If your AD uses groups that are member of another group, PRTG will **not** regard inherited implicit rights of the parent group and therefore refuse login for members of those groups.
- PRTG ignores AD information about **Organizational Units (OUs)**. These values cannot be read by PRTG. However, if you use the AD in an [auto-discovery group](#)^[285], you can restrict the search to computers that are part of an OU.
- PRTG does not support SSO (single sign-on).
- You can integrate only one AD domain into PRTG.

- PRTG does not support trusted domains or AD subdomains.
- For very large Active Directories, you will see an input field instead of a dropdown when you add or modify a user group. In this case, you can enter the group name only. PRTG will add the prefix automatically.
- A PRTG user account for an AD user is only created if this AD user successfully logs in to PRTG! So if you want to send [email notifications](#) to an AD user group (using the option "Send to User Group" in the notification settings), for example, by choosing the default notification "Email to all members of group [AD group name]", a member of this AD group has to log in to PRTG at least once to be able to receive an email notification. If you want to avoid these single logons of your AD group members to create user accounts, enter the email address of the AD group into the "Send to Email Address" field in the notification settings and choose "None" for the "Send to User Group" option.
- If you want to delete an AD group from PRTG (due to some changes to the AD, for example), you have to delete all users that are in this PRTG user group first. This is because AD users always have this group as their primary group, which cannot be changed.
- If you want to reflect changes to your AD in PRTG, you have to delete the AD user group and all members first. Then add the AD group anew. This is because PRTG does not synchronize with your AD automatically.

13.2 Application Programming Interface (API) Definition

The PRTG Application Programming Interface (API) enables you to access monitoring data and manipulate objects using HTTP requests, run your own written sensors and notifications, and implement Mini Probes.

-  An interactive documentation of the API is also integrated into your PRTG installation: [Login to the web interface](#) ¹⁶⁸ and select **Setup | PRTG API** from the main menu.



The following sections introduce the available options within the PRTG API:

- [HTTP API](#) ³⁶⁰⁷
- [Live Data](#) ³⁶¹⁰
- [Live Graphs](#) ³⁶²⁵
- [Historic Data](#) ³⁶²⁸
- [Object Manipulation](#) ³⁶³¹
- [Custom Sensors](#) ³⁶³⁷
- [Custom Notifications](#) ³⁶⁵⁸
- [Mini Probe API](#) ³⁶⁶⁰

The documentation that comes with your PRTG installation fits exactly the PRTG version you are using.

More

Knowledge Base: How can I share my self-written PRTG script/program with other PRTG users?

- <https://kb.paessler.com/en/topic/63737>

Knowledge Base: Where can I find PRTG Mini Probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

13.2.1 HTTP API

All calls to the PRTG HTTP API are performed by HTTP GET requests. The URLs consist of a path to the API function and some parameters.

- If you are accessing the API inside your secure LAN, you can simply use HTTP. In insecure environments (for example, when accessing your PRTG server across the internet), you should **use HTTPS requests** to make sure that your parameters and passwords are encrypted. This way all communication between the PRTG server and your client is SSL-encrypted.
- For every API call, the default limit of items is **500**. If you want to receive more items per call, add a **count=xxx** parameter with enough room for all sensors.
- Authentication with username and [passhash](#)³³⁰⁵ (or username and password) must always be included in each request. See section [Authentication](#)³⁶⁰⁷ for more information.
- All data in the GET parameters must be **UTF-8** encoded and **URL** encoded.

Here are two example API calls:

Examples

```
https://yourserver/api/table.xml?content=sensors&columns=sensor
```

or:

```
https://yourserver/api/table.xml?content=sensors&columns=sensor
```

The example URLs consist of the following elements:

- **yourserver**: the name of your PRTG server.
- **/api/table.xml**: addresses an API function. Here the function renders a table in Extensible Markup Language (XML) format.
- **content=sensors**: parameter for additional control. In this case, it includes all sensors in the table.
- **columns=sensor**: parameter for additional control. In this case, only the names of all sensors are shown in the table.

Authentication

All requests to the API are stateless, which means that there is no multi-step login process of an kind. The authentication with username and [passhash](#)³³⁰⁵ (or username and password) must always be included in each request by using the username and passhash (or username and password) parameters.

Examples

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&username=myuser&passw
```

or:

```
https://yourserver/api/table.xml?content=sensors&columns=sensor&username=myuser&passw
```

The example URLs now also contain the credentials for authentication purposes:

- **username=myuser&passhash=hash** (or **password=mypassword**)

You can request the passhash for an account with the following API call:

```
https://yourserver/api/getpasshash.htm?username=myuser&password=mypassword
```

- ⓘ Make sure that the username and password are URL encoded.

Versioning

Most XML replies from the API contain a **<version>** field that contains the program version and buildnumber of the server's PRTG installation. Your client must look at this version number and compare it to the version number that was used to develop the client. Do not accept version numbers older (smaller) than this one. You should display a warning to the user (or stop processing) if the version number differs by **0.1** or more (for example, version **18.1** vs. **18.2**, or version **17.x** vs. **18.x**). API conventions or parameters may have changed between versions.

- ⓘ Newer versions of the same major version of PRTG will reply to API calls just as previous versions have.

Error Handling

Depending on whether your API call was processed successfully or not, the PRTG server will reply with the following HTTP status codes:

HTTP STATUS CODE	MEANING	COMMENTS
200	OK	The API call was completed successfully, the XML response contains the result data.
302	Found	The API call was completed successfully and a new object was created (the redirection URL contains the new object id).
400	Bad Request	The API call could not be completed successfully. The XML response contains the error message.

HTTP STATUS CODE	MEANING	COMMENTS
401	Unauthorized	The username/password credentials cannot be accepted.

For 400 error codes, the error XML document will include the error message as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
  <prtg>
    <version>18.1.37.10127+</version>
    <error>Sorry, there is no object with the specified id.</error>
  </prtg>
```

More

Knowledge Base: How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

13.2.2 Live Data

You can access live data and live status data of objects using the PRTG Application Programming Interface (API).

 Authentication with username and [passhash](#)³³⁰⁵ (or username and password) must always be included in each PRTG API request. See section [Authentication](#)³⁶⁰⁷ for more information.

Getting One Single Property or Status of an Object

You can get the properties or settings of an object (name, hostname, url) as well as status information (lastvalue, downtime) using the following API calls:

Examples

Get an object property/setting:

```
/api/getobjectproperty.htm?id=objectid&name=propertyname
```

 For **propertyname**, look at the name of the INPUT fields while editing an object.

Get object status:

```
/api/getobjectstatus.htm?id=objectid&name=columnname
```

 For **columnname**, see section [Supported Output Columns \("columns=" Parameter\)](#)³⁶¹⁶.

The XML result looks like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<prtg>
  <version>18.1.37.10127+</version>
  <result>True</result>
</prtg>
```

Sensor Details

 You need the sensor ID to get details about a sensor. You can find the ID on the sensor's [overview](#)¹⁹⁸ tab or by hovering over a sensor in the device tree, for example.

Examples

Get details about a sensor in XML:

```
/api/getsensordetails.xml?id=sensorid
```

Get details about a sensor in JSON:

```
/api/getsensordetails.json?id=sensorid
```

Getting Property or Status of Multiple Objects

Most data that you can request from the API is available in data tables in XML, JSON, and CSV format (using XML format is recommended). The API function `/api/table.xml` is used to access data in tables. Here are some sample calls (URLs are shown without authentication parameters to improve readability).

 The example URLs only show the XML URLs. Use the API function `/api/table.csv` or the `output=csvtable` parameter to select CSV format, or `/api/table.json` to return JSON format.

Examples

A hierarchical list of all groups, devices, and sensors with their current status information:

```
/api/table.xml?content=sensortree
```

All sensors (with current status information):

```
/api/table.xml?content=sensors&columns=objid,group,device,sensor,status,message,last
```

All recent log entries:

```
/api/table.xml?content=messages&columns=objid,datetime,parent,type,name,status,message
```

 **sensortree** does not support JSON output.

You will have the easiest start if you use the [XML table query builder](#)  or click the XML icon that most data tables have in the PRTG web interface. Simply navigate to the information that you want to use, click the XML icon, and you will be taken to a URL that renders the content of the table in XML format. You can now use the URL as it is or change various parameters to suit your needs.

 For more information on possible raw message status values returned by table-based API calls, see the Knowledge Base article [Is there a list of log status values for the PRTG API?](#)

XML Table Query Builder

You can use the query builder tool to experiment with the API and to fine-tune your queries. You can find it in the web interface under **Set up | PRTG API**, section **Live Data**.

Output Data Format

XML data from the PRTG API contains the fields that you have requested in the **columns** parameter. In most cases, numerical values will be included twice: One field contains the value in human-readable format and an additional "RAW" field contains the value as a number, which is better suited for further processing and calculations.

Example

```
<status>Up</status>
<status_RAW>3</status_RAW>
<lastvalue>98 %</lastvalue>
<lastvalue_RAW>97.7583</lastvalue_RAW>
<message>Created.<br/>18.3.43.1360</message>
<message_RAW>Created. 18.3.43.1360</message_RAW>
```

- The **status** field shows the value **Up** (the according RAW value is **3**).
- The **lastvalue** field shows the value **98%** (the according RAW value is **97.7583**).
- The **message** field shows the text **Created.
18.3.43.1360** (the according RAW value is **Created. 18.3.43.1360**).

RAW Date/Time Format

For columns with date/time value, the RAW value is defined as follows: The integral part of a value is the number of days that have passed since Dec 30th, 1899. The fractional part of a value is a fraction of a 24-hour day that has elapsed. To find the fractional number of days between two dates, simply subtract the two values. Similarly, to increment a date and time value by a certain fractional number of days, add the fractional number to the date and time value.

Here are some examples of date/time RAW values and their corresponding dates and times:

RAW DATE/ TIME VALUE	DESCRIPTION
0	12/30/1899 00h00m (12:00 midnight)
2.75	1/1/1900 18h00m (6:00 pm)
35065	1/1/1996 00h00m (12:00 midnight)

Common Data Table Parameters

The following parameters are common to all data table API calls:

PARAMETER	DESCRIPTION	POSSIBLE VALUES
content	Selects what objects you want to have in your table	sensortree (JSON output not supported), devices, sensors, tickets, ticketdata, messages, values, channels, reports, storedreports, toplists
columns	Comma-separated list of columns per record	see Supported Output Columns ("columns=" Parameter)
output	Controls the output format	<ul style="list-style-type: none"> ▪ xml: default format (recommended) ▪ xmltable: an HTML table in XML format ▪ csvtable: comma-separated format ▪ html: HTML table ▪ json: JSON format ▪ jsontable: a table in JSON format
count	Maximum number of items (default 500)	1-50000
start	Start with this entry number (can be used with "count" to request the data page-by-page)	any

Filtering by Object ID

Add an ID parameter (for example, `id=1`) to the API URL to select a subset of items for the data table, for example, to reduce the amount of data transferred for each data table API call). The data table will only contain information for this object ID and its child objects.

 Some table types require an ID. If you omit the ID parameter or it has the value zero (0), all available objects will be used.

TABLE TYPE (CONTENT =)	ID REQUIRED OR OPTIONAL	DESCRIPTION	OBJECT TYPES ALLOWED FOR THE ID
sensortree	optional	You will only get a part of the tree (the object with the given ID and all child objects below it).  JSON output is not supported.	Probe or group
sensors devices	optional	You will only get the object with the given ID and all child objects below it.	Probe, group, or device
tickets messages	optional	You will only get tickets or logfile entries that are related to the object with the given ID or any child objects below it.	Any object
values channels	required	You will get the data values (or channels) of the sensor with the given ID.	Sensor
reports	not used	This data table will always include all reports.	n/a
storedreports	required	You will get a list of stored PDF files of the report selected by the ID.	Report
ticketdata	required	You will get the history of the ticket selected by the ID.	Ticket

Sorting and Advanced Filtering

There are various options to further filter and to sort the data for each data table API call:

PARAMETER	DESCRIPTION	POSSIBLE VALUES
filter_drel	Only include records younger than this setting  For content=messages and content=tickets only.	today, yesterday, 7days, 30days, 12months, 6months

PARAMETER	DESCRIPTION	POSSIBLE VALUES
filter_status	<p>Only include sensors with a specific status. Using multiple filter_status fields performs a logical OR.</p> <p> For content=sensors only.</p>	<p>Unknown=1, Collecting=2, Up=3, Warning=4, Down=5, NoProbe=6, PausedbyUser=7, PausedbyDependency=8, PausedbySchedule=9, Unusual=10, PausedbyLicense=11, PausedUntil=12, DownAcknowledged=13, DownPartial=14</p>
filter_tags	<p>Only include sensors with a specific tag. Using multiple filter_tag fields performs a logical OR.</p> <p> For content=sensors only.</p>	<p>@tag(tagname)</p>
filter_xyz	<p>Filters the data. (Samples: filter_type=ping, filter_favorite=1). Using multiple filter_xyz fields performs a logical OR.</p> <p>Filtering using columns is only possible for tree objects. You cannot use columns to filter objects like messages or tickets, for example. For content=tickets, you can use the special filter terms filter_status, filter_user, and filter_type (this corresponds to column tickettype).</p> <p>Like for messages, you can also use filter_drel, filter_dstart, and filter_dend.</p> <p> Multiple filters are not available for tickets.</p>	<p>filter_xyz where xyz is any column name used in the columns parameter</p> <p>Substrings: use filter_xyz=@sub (substring1,substring2)</p> <p>Values not equal/above/below: use filter_xyz=@neq(value), filter_xyz=@above (value), filter_xyz=@below(value)</p>

PARAMETER	DESCRIPTION	POSSIBLE VALUES
sortby	Sorts the data. If this parameter is omitted, the table will be sorted based on the first column. Add a leading "-" to reverse sort order. (Samples: sortby=name, sortby=lastvalue, sortby=-lastvalue, sortby=uptime)	Any column name used in the columns parameter.  Log tables with content=messages are always sorted by descending date.

Examples

Here are some samples for filtered API calls:

All sensors that are not up (with their current state and downtime information):

```
/api/table.xml?content=sensors&columns=objid,downtimesince,device,sensor,lastvalue,status
```

Fastest Ping sensors:

```
/api/table.xml?content=sensors&columns=objid,sensor,lastvalue,status,message&sortby=lastvalue
```

Log entries of the last 7 days for object id 2003:

```
/api/table.xml?content=messages&id=2003&start=0&filter_drel=7days&columns=objid,date
```

Supported Output Columns ("columns=" Parameter)

You can use the following column names for the **columns** parameter (separated by comma, for example, **columns=objid,name,type**).

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
objid	ID of the current object	all object tables
type	Displays the object type (group, device, report, etc.), or the sensor type (ping, http, etc.), or event type for tickets (relevant for ToDo tickets)	all object tables
name	Name of the object or channel. For log messages/tickets: the name of the related object.	all object tables, channels, messages, storedreports, toplists, tickets

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
	For stored reports: the name of the report file.	
tags	List of all tags (for tickets: tags for the related object). This includes tags from the object itself plus those inherited from parent objects.	all object tables
active	Displays true/false depending on whether an object is set to paused by a user (for tickets: related object). For notifications that are paused by schedule, it also displays the end of the schedule.	all object tables
downtime	Cumulated downtime of a sensor (displayed as percentage of uptime+downtime)	sensors
downtime	Cumulated downtime of a sensor (in minutes/hours)	sensors
downtimesince	Elapsed time since last UP of a sensor	sensors
uptime	Cumulated uptime of a sensor (displayed as percentage of uptime+downtime)	sensors
uptime	Cumulated uptime of a sensor (in minutes/hours)	sensors
uptimesince	Elapsed time since last DOWN of a sensor	sensors
knowntime	Sum of cumulated uptime and downtime of a sensor	sensors
cumsince	Timestamp when accumulation of uptimes/downtimes began	sensors
sensor	Name of the sensor	sensors, toplists

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
2 Live Data

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
interval	This displays the effective interval setting for a sensor	sensors
lastcheck	Timestamp of the last sensor result	sensors
lastup	Timestamp of the most recent UP status	sensors
lastdown	Timestamp of the most recent DOWN status	sensors
device	Name of the associated device	sensors, devices
group	Name of the associated group	sensors, devices, groups
probe	Name of the associated probe	sensors, devices, groups, probes
grpdev	Name of associated device and group separated by slash	sensors, devices
notifiesx	Number of each trigger type defined for this sensor tree object	probes, groups, devices, sensors
intervalx	Displays either 'inherited' or the current interval setting of that object	probes, groups, devices, sensors
access	Displays the access rights of the current user for a sensor tree object	probes, groups, devices, sensors
dependency	Displays the name of an associated dependency or 'parent'	probes, groups, devices, sensors
probegroupdevice	Complete object hierarchy with names of associated device, group, and probe separated by slash. If more than one group is in the object hierarchy, these are displayed with '..'	sensor, device, group, probe

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
status	<p>For sensor tree objects: status of the object (1=Unknown, 2=Scanning, 3=Up, 4=Warning, 5=Down, 6=No Probe, 7=Paused by User, 8=Paused by Dependency, 9=Paused by Schedule, 10=Unusual, 11=Not Licensed, 12=Paused Until, 13=Down Acknowledged, 14=Down Partial)</p> <p>For messages: category of the log message</p> <p>For tickets: status of ticket (open, resolved, closed)</p>	sensors, devices, groups, probes, messages, tickets
message	Detailed message of a sensor tree object (for example, last error of a sensor) or a history entry, log entry, ticket subject	sensors, devices, groups, probes, messages, tickets, ticketdata, history
priority	Displays the priority setting of a sensor tree object or the priority of a log entry/ticket	sensors, devices, groups, probes, messages, tickets
lastvalue	<p>Last sensor result value or channel values.</p> <p>When used with channels, the 'lastvalue_' has to be used to automatically display volumes and speed</p>	sensors, channels
upsens	<p>Number of sensors currently in UP state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
downsens	<p>Number of sensors currently in DOWN state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
downacksens	<p>Number of sensors currently in DOWN (ACKNOWLEDGED) state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
partialdownsens	<p>Number of sensors currently in PARTIAL DOWN state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
warnsens	<p>Number of sensors currently in WARNING state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
pausedsensors	<p>Number of sensors currently in a PAUSED state. This includes all PAUSED states (paused by user', 'paused by dependency, 'paused by schedule', etc.)</p>	all sensors, devices, groups, probes
unusualsens	<p>Number of sensors currently in UNUSUAL state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
undefinedsens	<p>Number of sensors currently in UNDEFINED state.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes
totalsens	<p>Number of sensors.</p> <p>Only the sensor itself or sensors in the hierarchy below the displayed object are counted</p>	all sensors, devices, groups, probes

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
value	Displays a channel value or a toplist value. Should only be used as 'value_', because then it will be expanded for all visible channels/toplist columns	values, topdata
coverage	Displays the sensor coverage of a time span in a value table	values
favorite	Displays an exclamation mark when the sensor tree object is marked as favorite	sensors, devices, groups, probes
user	Displays the user responsible for a history entry or the user (or user group) a ticket is assigned to	history, tickets, ticketdata
parent	Name of the parent object of the associated object of a log message	messages
datetime	Timestamp or timespan of an object (for tickets: last modification)	messages, tickets, ticketdata, values, history, storedreports, topidx
dateonly	Like datetime but only the date part	messages, tickets, history, values
timeonly	Like datetime but only the time part	messages, tickets, history, values
schedule	For sensor tree objects: displays the name of an associated schedule For reports: displays the report generation schedule	probes, groups, devices, sensors, reports
period	Displays the period of a report (day, week, etc.)	reports
email	Displays the email address of a report	reports

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
2 Live Data

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
template	Displays the template used by a report	reports
lastrun	Timestamp of the last generation of a report	reports
nextrun	Timestamp of the next generation of a report	reports
size	Size of a stored report	size of a stored report
minigraph	Numerical data for the minigraphs. Numbers are 5-minute averages for the last 24 hours (must be scaled to the maximum of the series). There are two datasets: " " separates measured value series and error series.	sensors
deviceicon	Device icon	devices
comments	Object comments For tickets: related object	all objects
host	Hostname or IP address	devices
devices	For probes: probe status (0=Disconnected, 1=Unauthorized, 2=Connected, 3=Banned, 4=Init) For groups: auto-discovery status	probes, groups
basetype	Object type (string)	all tree objects
baselink	URL of the object	all tree objects
icon	URL of the device icon	devices
parentid	ID of the parent object or ID of a ticket	all tree objects, tickets

COLUMN NAME	DESCRIPTION	CAN BE USED FOR
location	Location property (used in Geo Maps)	devices
fold	Sub-objects are folded up (true) or down (false) For tickets: user (or user group) to which a ticket is assigned read it since last change	probes, groups, tickets
groupnum devicenum	Number of groups/devices in a probe/group node	probes, groups
tickettype	Type of the ticket: user, notification, todo	tickets
modifiedby	User who edited the ticket most recently	tickets, ticketdata
actions	Types of all ticket edits	ticketdata
content	The text of the ticket that was added with the last edit	ticketdata

Requesting Current System Status

The following API calls are lightweight options to get status data like number of alarms or messages.

Examples

Current system status in XML format:

```
/api/getstatus.xml?id=0
```

Current system status in JSON format:

```
/api/getstatus.htm?id=0
```

All currently used sensor types in JSON format:

```
/api/sensortypesinuse.json
```

Current number of all sensor states:

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
2 Live Data

```
/api/gettreenodestats.xml
```

Requesting Current Ticket Status and Message

The following API calls return status and message of a ticket.

Examples

The status of a ticket:

```
/api/getticketstatus.htm?id=ticketid
```

The subject and assignee of a ticket:

```
/api/getticketmessage.htm?id=ticketid
```

More

Knowledge Base: How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

13.2.3 Live Graphs

You can use live sensor graphs from PRTG in other web pages using the PRTG API. PRTG renders graphs as PNG or SVG files. You can include them in other web pages.

i Authentication with username and [passhash](#)^[3305] (or username and password) must always be included in each PRTG API request. See section [Authentication](#)^[3607] for more information.

Examples

Live graph as PNG:

```
/chart.png?type=graph&width=300&height=160&graphid=2&id=0
```

Live graph as SVG:

```
/chart.svg?type=graph&width=300&height=160&graphid=2&id=0
```

i To switch between PNG and SVG, just change the file extension of `/chart` to `.png` or `.svg`.

i The URL does not start with `/api`. When placing these URLs on web pages, keep in mind that the URLs contain the account username and password/passhash. This can imply security concerns. We recommend that you set up a dedicated [read-only](#)^[158] user account in PRTG that is member of a dedicated user group, for example, that only has read rights for the root group and all underlying entries or, even better, only for the object IDs that are used for graph URLs.

Parameters for Live Graph URLs (`chart.png` or `chart.svg`)

PARAMETER	DESCRIPTION
type	Must be graph
graphid	Selects time span of the graph: 0=live, 1=last 48 hours, 2=30 days, 3=365 days
width	Width of the image in pixels
height	Height of the image in pixels
id	The object ID of the desired graph object. This is usually the ID of a sensor.
graphstyling	Allows control of some graph styles: <ul style="list-style-type: none"> Display legend: <code>graphstyling=showLegend%3D%271%27</code>

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ▪ Hide legend: <code>graphstyling=showLegend%3D%270%27</code> ▪ Control font size: <code>graphstyling=baseFontSize%3D%27XX%27</code> (XX is the font size) ▪ Control legend and font size at the same time: <code>graphstyling=showLegend%3D%271%27+baseFontSize%3D%275%27</code>
<code>bgcolor</code>	<p>Background color of the PNG image, for example, <code>#ffffff</code>. This affects the area that surrounds the graph.</p> <p> The value must be URL-encoded, for example, <code>%23ffffff</code>.</p>
<code>plotcolor</code>	<p>Color of the graph's plot area, for example, <code>#ffffff</code>. This affects the whole area within the graph box.</p> <p> The value must be URL encoded, for example, <code>%23ffffff</code>.</p>
<code>plotcolor1</code>	<p>Alternating color of the graph's plot area, for example, <code>#ffffff</code>. This affects the tiles within the graph box alternating with <code>plotcolor2</code>. The result is a striped graph box.</p> <p> The value must be URL encoded, for example, <code>%23ffffff</code>.</p> <p> This parameter is overwritten when using the parameter <code>plotcolor</code>.</p>
<code>plotcolor2</code>	<p>Alternating color of the graph's plot area, for example, <code>#ffffff</code>. This affects the tiles within the graph box alternating with <code>plotcolor1</code>. The result is a striped graph box.</p> <p> The value must be URL encoded, for example, <code>%23ffffff</code>.</p> <p> This parameter is overwritten when using the parameter <code>plotcolor</code>.</p>
<code>gridcolor</code>	<p>Color of gridlines in the graph's plot area, for example, <code>#ffffff</code>. This affects the horizontal and vertical lines within the graph box.</p> <p> The value must be URL encoded, for example, <code>%23ffffff</code>.</p>
<code>hide</code>	<p>Do not show defined channels in the graph. Use the ID of a channel to hide it. For example, use <code>hide=-4</code> to not show the downtime channel in the graph. To hide more than one channel, use commas to separate the IDs.</p>

Retrieving Chart Legends (JSON)

You can show the legend of a sensor graph (channel IDs, colors, units, channel names) in JSON format.

Example

Chart legend in JSON format:

```
/api/chartlegend.json?id=sensorid
```

More

Knowledge Base: How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

13.2.4 Historic Data

You can download the historic monitoring data for one sensor in XML or CSV format using the following API calls. You can either request the results of each single monitoring request (called raw data) or you can let PRTG calculate averages of the data (for example, hourly or daily averages).

To avoid potential server overload, the number of requestable values per API call is limited by means of automatic averaging as follows:

MINIMUM LEVEL OF DETAIL (AVERAGE INTERVAL)	MAXIMUM TIMEFRAME PER API CALL
Raw data (all single monitoring requests)	For up to 40 days per API request
60 minutes/1 hour averages	40 to 500 days per API request

i If you try to use a larger time span than 500 days, PRTG will reduce it to 365 days automatically.

i API calls for historic data are limited to 5 requests per minute.

API Calls for Historic Data

i Authentication with username and [passhash](#) (or username and password) must always be included in each PRTG API request. See section [Authentication](#) for more information.

The API calls for historic data tables look like this:

Examples

XML:

```
/api/historicdata.xml?id=objectid&avg=0&sdate=2018-01-20-00-00-00&edate=2018-01-21-00-00-00
```

CSV:

```
/api/historicdata.csv?id=objectid&avg=0&sdate=2018-01-20-00-00-00&edate=2018-01-21-00-00-00
```

JSON:

```
/api/historicdata.json?id=objectid&avg=0&sdate=2018-01-20-00-00-00&edate=2018-01-21-00-00-00
```

i You must supply the object ID of a sensor as well as a start date/time **sdate** and end date/time **edate**.

- i** If you use the JSON call, additionally provide the parameter **usecaption=1** to get more information than just the raw data table.

API Call for Historic Graphs

Historic graphs are also available (in PNG format):

Example

PNG:

```
/chart.png?id=objectid&avg=15&sdate=2018-01-20-00-00-00&edate=2018-01-21-00-00-00&wic
```

Common Parameters for Historic Data API Calls

The following parameters can be used for the graphs and the data tables:

PARAMETER	DESCRIPTION	POSSIBLE VALUES
id	ID of the specific sensor	integer value
sdate	Start of the time span (date and time)	yyyy-mm-dd-hh-mm-ss
edate	End of the time span (date and time)	yyyy-mm-dd-hh-mm-ss
avg	Average interval in seconds; use 0 to download raw data (= results of all single monitoring requests)	integer value
width/height	Width and height of the graph in pixels	integer value
graphstyling	baseFontSize='x' sets the size of the font showLegend='x' enables (1) or disables (0) the graph legend	baseFontSize='x'% 20showLegend='x'

Historic Data Query Builder

You can also use the [historic data function](#) ^[204] to manually generate and analyze historic sensor data via the PRTG web interface.

More

Knowledge Base: How can I export historic data from the PRTG API?

- <https://kb.paessler.com/en/topic/76768>

Knowledge Base: How can I export raw sensor data automatically from PRTG?

- <https://kb.paessler.com/en/topic/343>

13.2.5 Object Manipulation

You can use the following functions to manipulate existing objects (URLs are shown without username/passhash to improve readability).

Here are quick links for ease of use.

- [Changing Object Settings](#) 
- [Switch Inheritance Off/On](#) 
- [Changing Properties of Channels](#) 
- [Pausing/Resuming](#) 
- [Error Handling, Rescanning](#) 
- [Rescanning, Triggering Auto-Discovery](#) 
- [Reordering Objects in the Sensor Tree](#) 
- [Report-related](#) 
- [Notification-related](#) 
- [Adding/Deleting Objects](#) 
- [Duplicating Sensors and Changing Clone Settings](#) 
- [Setting Geo Location](#) 

Changing Object Settings

 Authentication with username and [passhash](#)  (or username and password) must always be included in each PRTG API request. See section [Authentication](#)  for more information.

Examples

Rename an object:

```
/api/rename.htm?id=objectid&value=newname
```

Set priority of an object (valid values for x are 1 to 5):

```
/api/setpriority.htm?id=objectid&prio=x
```

Change properties of objects:

```
/api/setobjectproperty.htm?id=id_of_object&name=property_name&value=new_value
```

 This function can change most string and number properties of objects (names, numerical values, OIDs, etc.) and should be used with caution. The **property_name** parameter can be discerned by opening the **Settings** page of an object and looking at the HTML source of the INPUT fields. For example, the INPUT field for the tags of an object has the name **tags_**. Leave away the **_** and use the rest (**tags**) as a value for the **property_name** parameter.

Switch Inheritance Off/On

This API call sets the "inherit" setting of objects (location, credentials, compatibility options, proxy settings, scanning interval, access rights, channel unit). In general, this works like changing properties for any other object.

Example

Replace the parameter **inheritType** with the name of the inheritance type:

```
/api/setobjectproperty.htm?id=id_of_object&name=inheritType_&value=0_or_1
```

i This internal name must be followed by an underscore (_), in contrast to changing properties above. Use the value **0** for switching off inheritance, and **1** for switching on inheritance. For example, the inheritance type for the scanning interval setting has the name **intervalgroup_**; thus, this specific part in the URL is **&name=intervalgroup_&value=0** (switches off inheritance for scanning interval).

i This call does not work with the schedules, dependencies, and maintenance window.

Changing Properties of Channels

With this API call, you can change a sensor's [channels settings](#)³¹⁶⁰. In general, this works like changing properties of any other object. To set channel properties via the API, you need to provide

- the ID of a sensor (parameter id)
- a subtype (channel for channels), and
- a subid (ID of the channel you want to edit).

Example: Enabling and Setting Limits for Channels

Enable limits for channels:

```
/api/setobjectproperty.htm?id=sensorid&subtype=channel&subid=0&name=limitmode&value=1
```

i You have to enable the limits for a channel before you can set limits.

Set limits for channels:

```
/api/setobjectproperty.htm?id=sensorid&subtype=channel&subid=0&name=limitmaxerror&value=25
```

For example, the following API call sets the upper error limit of a channel with the ID 0 of a sensor with the ID 2970 to the value 25.

```
/api/setobjectproperty.htm?id=2970&subtype=channel&subid=0&name=limitmaxerror&value=25
```

i For toplists, you can use the subtype **toplist** to change the properties. When using this subtype, **subid** is the ID of a toplist.

Pausing/Resuming

Examples

Pause a sensor or object indefinitely:

```
/api/pause.htm?id=objectid&pausemsg=yourmessage&action=0-00
```

Pause a sensor or object for x minutes:

```
/api/pauseobjectfor.htm?id=objectid&pausemsg=yourmessage&duration=x
```

i The pause message is optional. You can leave out the parameter **&pausemsg=yourmessage** if you do not want to display a message.

Pause and simulate a down status for a sensor:

```
/api/simulate.htm?id=objectid&action=1
```

Resume monitoring of a sensor or object:

```
/api/pause.htm?id=objectid&action=1
```

Error Handling (Acknowledge Alarm)

Example

Acknowledge a down status:

```
/api/acknowledgealarm.htm?id=objectid&ackmsg=yourmessage
```

Rescanning, Triggering Auto-Discovery

Examples

Scan a sensor now:

```
/api/scannow.htm?id=objectid
```

Run an auto-discovery for an object:

```
/api/discovernow.htm?id=objectid&template=filename
```

i Template for auto-discovery is optional. You can leave out the parameter **&template=filename** to run the auto-discovery with the options defined in the object's settings.

i If you use a template, provide the whole filename including file extension surrounded by double quotes and encode whitespaces, if necessary. Example: **&template="Linux%20SNMP.odt"**

Reordering Objects in the Sensor Tree

Example

Move an object in the sensor tree (x can be **up**, **down**, **top**, **bottom**):

```
/api/setposition.htm?id=objectid&newpos=x
```

Report-related

Example

Add a group, device, or sensor to a report:

```
/api/reportaddsensor.htm?id=reportid&addid=objectid
```

Notification-related

Example

Test a notification:

```
/api/notificationtest.htm?id=objectid
```

Adding/Deleting Objects

Adding and deleting objects in your PRTG configuration is the most complex and potentially most "dangerous" process when using the API. Keep in mind that add/delete activity is much better guided in the normal web interface with more warnings and alerts.

-  We recommend that you use the web interface for adding and deleting objects if possible.

Deleting Objects

-  API calls to the delete function immediately delete the referenced object including all subobjects, if there are any. For example, deleting a group deletes all its devices and sensors! There is no way to undo a deletion so use this function with care.

Example

Delete an object:

```
/api/deleteobject.htm?id=objectid&approve=1
```

Adding Objects

Adding completely new objects from scratch is not supported via the API due to the complexity of object creation and its parameters. To add new objects to PRTG, create a "master" object that will be cloned into new objects.

Examples

Duplicate a group:

```
/api/duplicateobject.htm?id=id_of_group_to_clone&name=new_name&targetid=id_of_target_
```

Duplicate a device:

```
/api/duplicateobject.htm?id=id_of_device_to_clone&name=new_name&host=new_hostname_or_
```

Duplicate a sensor:

```
/api/duplicateobject.htm?id=id_of_sensor_to_clone&name=new_name&targetid=id_of_target_
```

i If the **duplicateobject** succeeds, the PRTG server will reply with a redirect to the URL of the new object (for example, **/sensor.htm?id=1234**), so your application should parse the new object ID from this URL.

i When an object is cloned, it will initially be set to "paused" so you have the chance to edit parameters as desired. You must resume it with an API call afterwards.

Duplicating Sensors and Changing Clone Settings

The following process duplicates a sensor, changes some settings, and then starts monitoring:

Example

Duplicate the sensor (the server replies with a redirect to the new object's webpage, for example **/sensor.htm?id=10214**, parse id **10214** from the URL):

```
/api/duplicateobject.htm?id=2002&name=mynewsensor&targetid=2001
```

Rename the new sensor:

```
/api/setobjectproperty.htm?id=10214&name=name&value=anothernewname
```

Change the OID (in this example for an [SNMP Custom sensor](#)¹⁹⁴⁹):

```
/api/setobjectproperty.htm?id=10214&name=oid&value=1.2.3.4.5.6.7
```

Resume monitoring for the new sensor:

```
/api/pause.htm?id=10214&action=1
```

Setting Geo Location

You can set the location of any object via an API call. Provide the object ID together with parameters for location and/or longitude and latitude.

If only the location parameter is given, the PRTG core server will execute the geo location lookup (this can take up to three minutes). Provide the name of the location, for example, **New York**. It will be shown in the **Location** settings, no matter the longitude/latitude.

If the longitude/latitude parameter is given, the marker in the map will be set to this position, no matter of the location parameter. Provide longitude and latitude separated by a comma, for example **-73.998672,40.714728**.

Example

Set the geo location of an object:

```
/api/setlonlat.htm?id=objectid&location=name_of_object_location&lonlat=longitude,latitude
```

More

Knowledge Base: How can I use the PRTG Application Programming Interface (API)?

- <https://kb.paessler.com/en/topic/593>

13.2.6 Custom Sensors

Custom sensors allow a number of monitoring tasks to be performed that go far beyond the standard sensor set. Apart from parameterized versions of SNMP, Packet Sniffer, and NetFlow sensors, you can create your own sensors using WQL or Python, by compiling an EXE file, using any Windows software development tool, and you can request any REST API that returns JSON or XML and map the results to sensor channels.

The following documentation describes the custom [EXE/Script](#)^[834], [Python Script](#)^[1597], and [SSH Script](#)^[2607] sensors. The defined XML and JSON formats for the advanced sensors are also used for advanced HTTP data sensors and the [REST Custom](#)^[1646] sensor.

 For more information about custom sensors based on SNMP, WMI, Packet Sniffing, and xFlow, see the respective [custom sensor types](#)^[3152].

 For each sensor interval, PRTG can run an external process. The process can be a Windows EXE file, or a DLL, BAT, CMD, VBS, or PowerShell file, as well as a Python or SSH script.

Here are quick links for ease of use.

- [Standard and Advanced EXE/Script Sensor](#)^[3637]
- [Standard and Advanced SSH Script Sensor](#)^[3638]
- [Interface Definition for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors](#)^[3638]
- [Return Values for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors](#)^[3639]
- [Standard EXE/Script Sensor](#)^[3639]
- [Standard SSH Script Sensor](#)^[3640]
- [Advanced Script, HTTP Data, and REST Custom Sensors](#)^[3641]
- [Advanced Script, HTTP Data, and REST Custom Sensors: Elements](#)^[3642]
- [Interface Definition for DLL Sensors](#)^[3653]
- [Command Line Parameters](#)^[3654]
- [Escape Special Characters and Whitespaces in Parameters](#)^[3655]
- [Environment Values](#)^[3656]
- [PRTG Script World](#)^[3656]

Standard and Advanced EXE/Script Sensor

 You must create the sensor as a file and place it in a specific folder on the system running the PRTG probe. This means that if you are using remote probes, the files must be copied to the remote system, in a PRTG cluster setup on each cluster node.

Place executables (.EXE, .DLL), batchfiles (.CMD, .BAT), VBS scripts (.VBS), or PowerShell scripts (.PS1) into a subfolder of the PRTG program directory. For the standard [EXE/Script sensor](#)^[834], this is the following subfolder of your PRTG program directory:

```
Custom Sensors\EXE
```

If your executable or script returns XML or JSON, you will use it with the [EXE/Script Advanced sensor](#)^[847]. In this case, store your file in the following subfolder of the PRTG program directory:

```
Custom Sensors\EXEXML
```

You will find a sample set of demo sensors in these folders, too. As soon as a file is placed into the folders mentioned above, you can create your own custom EXE sensor and select the new file from the list of files.

The probe will then execute the file on the probe system using the account configured for the PRTG probe service ("system" is the default). The local probe will run the file on the local PRTG core server system. For remote probes, the file will actually run on the remote system.

- ⚠ If your custom sensor code relies on other files (for example, DLLs, .NET framework, Windows PowerShell) you must copy/install these files on the probe machine manually!
- ⚠ EXE sensors will fail if they attempt to open any graphical user interface windows using the Win32 APIs. This is not allowed for processes that are started by a system service.

Standard and Advanced SSH Script Sensor

- ⓘ You must create the sensor as an SSH script and place it in a specific folder on the target system running your Linux/Unix installation where the script will be executed.

Place your SSH script files for the standard [SSH Script sensor](#)^[2607] in the following directory of the target system:

```
/var/prtg/scripts
```

If your SSH script returns XML or JSON, you will use it with the [SSH Script Advanced sensor](#)^[2622]. In this case, store your file in the following directory of the target system:

```
/var/prtg/scriptsxml
```

As soon as a file is placed into the respective folder, you can create your own SSH script sensor and select the new script file from the list of scripts.

- ⓘ With each scanning interval, PRTG will execute the script on the target system and receive the result as a sensor result.

Interface Definition for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors

Every time the sensor is run, the selected file is executed. The string entered in the **Parameters** field of the sensor's settings is used as command line (you can use placeholders, see [Command Line Parameters](#)^[3654]). The executable file must send the results to the Standard OUT. For the format of returned data, see below.

- ⓘ If the EXE does not return control to the PRTG process, it is killed as soon as the timeout value set for this sensor is reached.

You can test the EXE file you want to use for the sensor very easily on the command line (cmd.exe). Simply start the EXE file and pipe the results into a file.

Example

```
sensorexex parameter > result.txt
```

The results are written into the file **result.txt** and you can check the results with notepad or any other text editor.

Remarks

- For PowerShell scripts, make sure that they may be executed by either signing the files or changing the security policy for Powershell.exe accordingly.
- In SSH scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings in the **Parameters** field of the sensor's settings.
- The API interface for custom EXE sensors is compatible with the custom EXE sensors provided by PRTG Network Monitor.

Return Values for EXE/BAT/CMD/VBS/PowerShell/SSH Sensors

The expected return values are different, depending on the type of [EXE/Script sensor](#)^[834] used. The standard sensor needs a simple **value:message** pair; the [EXE/Script Advanced sensor](#)^[847] processes an XML or JSON return value. When using the standard [SSH Script sensor](#)^[2607], it will expect **returncode:value:message** as result. See details below.

Standard EXE/Script Sensor

The returned data for standard EXE/Script sensors must be in the following format:

```
value:message
```

i Value has to be a 64-bit integer or float. It will be used as the resulting value for this sensor (for example, bytes, milliseconds) and stored in the database. The message can be any string (maximum length: 2000 characters).

The exit code of the EXE has to be one of the following values:

VALUE	DESCRIPTION
0	OK
1	WARNING

VALUE	DESCRIPTION
2	System Error (for example, a network/socket error)
3	Protocol Error (for example, web server returns a 404)
4	Content Error (for example, a web page does not contain a required word)

Standard SSH Script Sensor

The returned data for standard SSH Script sensors must be in the following format:

```
returncode:value:message
```

i Value has to be a 64-bit integer or float. It will be used as the resulting value for this sensor (for example, bytes, milliseconds) and stored in the database. The message can be any string (maximum length: 2000 characters).

The SSH script **returncode** has to be one of the following values:

VALUE	DESCRIPTION
0	OK
1	WARNING
2	System Error (for example, a network/socket error)
3	Protocol Error (for example, web server returns a 404)
4	Content Error (for example, a web page does not contain a required word)

Advanced Script, HTTP Data, and REST Custom Sensors

The returned data for the [EXE/Script Advanced](#), [Python Script Advanced](#), [SSH Script Advanced](#), [HTTP Push Data Advanced](#), [HTTP Data Advanced](#), and [HTTP IoT Push Data Advanced](#) sensors must be in XML or JSON format, the REST configuration file for the [REST Custom sensor](#) must be available as JSON template. Most parameters have a default value and are not required.

The following minimum examples leave most parameters to their default values and return two static channel values.

Examples

XML Return Format: Minimum Example:

```
<prtg>
  <result>
    <channel>First channel</channel>
    <value>10</value>
  </result>
  <result>
    <channel>Second channel</channel>
    <value>20</value>
  </result>
</prtg>
```

To return an error, the XML format is:

```
<prtg>
  <error>1</error>
  <text>Your error message</text>
</prtg>
```

JSON Return Format: Minimum Example

```
{
  "prtg": {
    "result": [
      {
        "channel": "First channel",
        "value": "10"
      },
      {
        "channel": "Second channel",
        "value": "20"
      }
    ]
  }
}
```

To return an error, the JSON format is:

```
{
  "prtg": {
    "error": "1",
    "text": "Your error message"
  }
}
```

i You can find a more detailed demo script for the EXE/Script Advanced sensor in the **Custom Sensors\EXEXML** subfolder of your PRTG installation. You will find demo files for other sensors in the **Custom Sensors** folder as well.

Advanced Script, HTTP Data, and REST Custom Sensors: Elements

You can optionally define the encoding of your XML file at the beginning of the document. For example, to define UTF-8, you would use:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

The following elements can be used in the section between **<result>** and **</result>**. In each section, you can return one sensor channel. You may define a maximum of **50** sensor channels.

i If you exceed this limit, PRTG will try to display all sensor channels. However, be aware that this is an unsupported procedure and you will experience limited usability and performance.

i The tag names are not case-sensitive. For example, "VALUE" and "value" can both be used.

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<Channel>	Yes	Name of the channel as displayed in user interfaces.  This parameter is required and must be unique for the sensor.	Any string
<Value>	Yes	The value as integer or float.  Make sure the <Float> setting matches the kind of value provided. Otherwise PRTG will show 0 values.	Integer or float value
<Unit>	No	The unit of the value. Default is Custom. This is useful for PRTG to be able to convert volumes and times.	BytesBandwidth BytesDisk Temperature Percent TimeResponse TimeSeconds Custom Count CPU: This is a % unit that is accounted to the CPU load in index graphs. BytesFile SpeedDisk SpeedNet TimeHours
<CustomUnit>	No	If Custom is used as unit, this is the text displayed behind the value.	Any string (keep it short)

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
6 Custom Sensors

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<SpeedSize> <VolumeSize>	No	Size used for the display value. For example, if you have a value of 50000 and use Kilo as size, the display is 50 kilo #. Default is One (value used as returned). For the Bytes and Speed units, this is overridden by the setting in the user interface.	One Kilo Mega Giga Tera Byte KiloByte MegaByte GigaByte TeraByte Bit KiloBit MegaBit GigaBit TeraBit
<SpeedTime>	No	See above, used when displaying the speed. Default is Second.	Second Minute Hour Day
<Mode>	No	Select if the value is an absolute value or counter. Default is Absolute.	Absolute Difference
<Float>	No	Define if the value is a float. Default is 0 (no). If set to 1 (yes), use a dot as decimal separator in values.  Define decimal places with the <DecimalMode> element.	0 (= no, integer) 1 (= yes, float)

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<DecimalMode>	No	<p>Init value for the Decimal Places option. If 0 is used in the <Float> element (use integer), the default is Auto; otherwise (for float) the default is All.</p> <p> You can change this initial setting later in the sensor's channel settings³¹⁸⁰.</p>	<p>Auto</p> <p>All</p>
<Warning>	No	<p>If enabled for at least one channel, the entire sensor is set to "Warning" status. Default is 0 (no).</p>	<p>0 (= no)</p> <p>1 (= yes)</p>
<ShowChart>	No	<p>Init value for the Show in Graphs option. Default is 1 (yes).</p> <p> The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁸⁰.</p>	<p>0 (= no)</p> <p>1 (= yes)</p>
<ShowTable>	No	<p>Init value for the Show in Tables option. Default is 1 (yes).</p>	<p>0 (= no)</p> <p>1 (= yes)</p>

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitMaxError>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define an upper error limit for the channel. If enabled, the sensor will be set to a "Down" status if this value is overrun and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section. While a sensor shows a "Down" status triggered by a limit, it will still receive data in its channels.</p>	Integer

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitMaxWarning>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define an upper warning limit for the channel. If enabled, the sensor will be set to a "Warning" status if this value is overrun and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section. While a sensor shows a "Down" status triggered by a limit, it will still receive data in its channels.</p>	Integer

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitMinWarning>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define a lower warning limit for the channel. If enabled, the sensor will be set to a "Warning" status if this value is undercut and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section. While a sensor shows a "Down" status triggered by a limit, it will still receive data in its channels.</p>	Integer

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitMinError>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define a lower error limit for the channel. If enabled, the sensor will be set to a "Down" status if this value is undercut and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section. While a sensor shows a "Down" status triggered by a limit, it will still receive data in its channels.</p>	Integer

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitErrorMsg>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define an additional message. It will be added to the sensor's message when entering a "Down" status that is triggered by a limit.</p>	Any string
<LimitWarningMsg>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define an additional message. It will be added to the sensor's message when entering a "Warning" status that is triggered by a limit.</p>	Any string

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<LimitMode>	No	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define if the limit settings defined above will be active. Default is 0 (no; limits inactive). If 0 is used the limits will be written to the sensor channel settings as predefined values, but limits will be disabled.</p> <p>i This setting will be considered only on the first sensor scan, when the channel is newly created; it is ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p>	<p>0 (= no) 1 (= yes)</p>

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
 6 Custom Sensors

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<ValueLookup>	No	Define if you want to use a lookup file (for example, to view integer values as status texts). Enter the ID of the lookup file you want to use, or omit this element to not use lookups.  This setting will be considered only on the first sensor scan, when the channel is newly created; it is ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings ³¹⁶⁰ .	Any string
<NotifyChanged>	No	If a returned channel contains this tag, it will trigger a change notification that you can use with the Change Trigger ³¹⁸⁰ to send a notification.	No content required

The following elements can be used in the section between <prt g> and </prt g>, outside the <result> section.

 The tag names are not case-sensitive. For example, "TEXT" and "text" can both be used.

TAG (CASE INSENSITIVE)	MANDATORY	DESCRIPTION	POSSIBLE CONTENT
<Text>	No	Text the sensor returns in the Message field with every scanning interval. There can be one message per sensor, regardless of the number of channels. Default is OK .  This element has to be provided outside of the <result> element.	Any string; Maximum length: 2000 characters
<Error>	No	If enabled, the sensor will return an error status. This element can be combined with the <Text> element in order to show an error message. Default is 0 .  This element has to be provided outside of the <result> element. A sensor in this error status cannot return any data in its channels; if used, all channel values in the <result> section will be ignored.	0 (= no) 1 (= yes, set sensor to error; ignore <result> section)

-  Each run (sensor scan) may return either any number of channels (<result>...</result>) or one error response. It is not possible to mix result and error entries.
-  You can either write the XML output to standard OUT line by line, or give back the entire expression in one line without breaks.

Interface Definition for DLL Sensors

Every time the sensor is to be checked, a function in the selected DLL file is called. The DLL must export one function:

```
function perform(para,msg:pchar):integer; stdcall;
```

para and **msg** are zero-terminated strings. The allocated buffer for **msg** is 255 bytes, the DLL must make sure that fewer bytes are returned. **Msg** must be in the following format:

```
value:message
```

Value has to be an 32-bit integer and will be used as the resulting value for this sensor (for example, bytes, milliseconds, etc.), **message** can be any string and will be stored in the database.

 The integer return value of the perform function has to conform to the same rules as the EXE exit code mentioned above.

 If the function call in the DLL does not return control, it could block the whole PRTG system. Make sure to handle your own timeouts and build in a reliable error management. For this reason EXE sensors are recommended.

Command Line Parameters

In the **parameter** field you can use the following placeholders:

PLACEHOLDER	DESCRIPTION
%sensorid	The ID of the EXE/Script sensor.
%deviceid	The ID of the device the sensor is created on.
%groupid	The ID of the group the sensor is created in.
%probeid	The ID of the probe the sensor is created on.
%host	The IP address/DNS name entry of the device the sensor is created on.
%device	The name of the device the sensor is created on.
%group	The name of the group the sensor is created in.
%probe	The name of the probe the sensor is created on.

PLACEHOLDER	DESCRIPTION
%name or %sensor	The name of the EXE/Script sensor.
%windowsdomain	The domain for Windows access (may be inherited from parent).
%windowsuser	The user name for Windows access (may be inherited from parent).
%windowspassword	The password for Windows access (may be inherited from parent).
%linuxuser	The user name for Linux access (may be inherited from parent).
%linuxpassword	The password for Linux access (may be inherited from parent).
%snmpcommunity	The community string for SNMP v1 or v2 (may be inherited from parent).

 You need to escape special characters and whitespaces in your parameters and surround them with double quotes. See section [Escape Special Characters and Whitespaces in Parameters](#)²⁶¹⁹ for details. In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ".", "_", "-", "=", and "/" outside of quoted strings.

 See section [Inheritance of Settings](#)¹³⁷ for more information on inherited settings.

Escape Special Characters and Whitespaces in Parameters

 You need to escape special characters in parameters that you pass to an executable or script and surround them with quotation marks to make sure the characters are interpreted correctly. Especially PowerShell scripts require adequate escaping so that the parameters are passed in a valid PowerShell syntax. To make escaping easy and secure, PRTG automatically does most of the escaping for you.

Please follow these rules to escape special characters and whitespaces in the parameters fields:

- Use quotes for parameters that contain whitespaces.

```
-name "Mr John Q Public"
-name 'Mr John Q Public'
```

- Use double quotes for parameters that contain single quotes.

```
-name "Mr 'John Q' Public"
```

- Use single quotes for parameters that contain double quotes.

```
-name 'Mr "John Q" Public'
```

- Use a backslash (\) to escape and pass a literal double quote.

```
-name pub\"lic
```

- Use double quotes for parameters that contain double **and** single quotes and escape double quotes.

```
-name "pu'b\"lic"
```

In Secure Shell (SSH) scripts, you can use alphanumeric characters and the special characters ":", "_", "-", "=", and "/" outside of quoted strings.

 We recommend that you do not pass passwords in parameters. Use PRTG placeholders instead. See section [Custom Sensors](#) for details.

Environment Values

If the **Set placeholders as environment values** option is enabled in the sensor's settings, the values of all placeholders available for [command line parameters](#) are additionally provided as "Environment Variables" during runtime, so you can use them in your executable or script file. The variables' names are the same as for placeholders mentioned above, with the prefix **prtg_** and without the % character. For example, refer to the sensor's own name by using the variable **prtg_name**.

Additionally, the following variables are available:

VARIABLE	DESCRIPTION
prtg_version	The version number of your PRTG installation.
prtg_url	The IP address/DNS name of your PRTG installation.
prtg_primarychannel	The ID of the sensor's current primary channel (1 if not set).

PRTG Script World

Find useful scripts for custom sensors in the [PRTG Script World](#), written by dedicated PRTG customers around the world and Paessler!

More

You can find sample projects for these custom sensors and more information about custom scripts here:

- In the **PRTG Network Monitor\custom sensors\EXE** subfolder of your PRTG installation.
- In the Knowledge Base on the Paessler website at <https://kb.paessler.com> (tag custom-script-exe).
- This Knowledge Base article will help you set up your PowerShell sensors: [Guide for PowerShell Based Custom Sensors](#).

13.2.7 Custom Notifications

In addition to the various standard methods for notifications, you can also define your own notifications that can trigger desired actions. The possibilities of these notifications go far beyond just sending out messages, because you can perform almost any action you like whenever the notification is triggered.

The following documentation describes these custom notifications. Different notification methods can also be combined in one notification.

 For more general information about notifications based on email, messaging, and others, see section [Notifications](#)³²¹⁶.

Execute HTTP Action

This notification method executes a GET request or sends any POST, PUT, or PATCH data to a custom URL. You can execute specific actions on a web server or control any web service that accepts commands via one-time HTTP requests. Whenever a notification of this kind is triggered, the HTTP action is sent.

With this method, you can also call any API function of the PRTG web interface. For example, you can set PRTG to automatically pause a sensor, or acknowledge an alarm.

 Authentication with username and [passhash](#)³³⁰⁵ (or username and password) must always be included in each PRTG API request. See section [Authentication](#)³⁶⁰⁷ for more information.

Examples

To automatically pause the sensor that triggers the notification, enter the following HTTP action:

```
http://yourserver/api/pause.htm?id=%sensorid&action=0&username=myuser&password=mypas
```

To use the notification to automatically acknowledge the alarm that triggered it, enter this HTTP action:

```
http://yourserver/api/acknowledgealarm.htm?id=%sensorid&ackmsg=Auto-Acknowledged&use
```

 For more information about authentication within the URL and for other possible actions you can configure, see sections [HTTP API](#)³⁶⁰⁷ and [Object Manipulation](#)³⁶³¹.

Execute Program

With this notification method, you can execute a script or a program as an external process. It can be a Windows executable file or a BAT, CMD, or PowerShell file. You can use EXE, COM, BAT, CMD, VBS, or PS1 files.

 You must create the notification as a file and place it in a specific folder on the PRTG core server system (in a cluster, copy the files to every node).

Place executables (.EXE, .COM), batch files (.CMD, .BAT), VBS scripts (.VBS), or PowerShell scripts (.PS1) into the folder:

```
\Notifications\EXE
```

As soon as a file is placed into the folder, you can create or edit your own custom execute program notification and select the new file from the list of files. You can also enter start parameters and use PRTG placeholders for this.

Notes

- PRTG will execute the file on the local PRTG core server system using the account configured for the PRTG core server service ("system" is the default).
- If your custom notifications code relies on other files (for example, DLLs, .NET framework, or Windows PowerShell), you must copy/install these files on the PRTG core server machine manually!
- Make sure the return code of the executable is 0 (zero). Otherwise PRTG assumes something went wrong with the notification and will try to send it up to 3 times.
- When running PRTG in a cluster, copy the respective files to every single node to make sure the notification also works when the primary master is not reachable.
- EXE notifications will fail if they attempt to open any graphical user interface windows using the Win32 APIs (this is not allowed for processes that are started by a system service).

Placeholders

 For more information about the placeholders you can use, see the Paessler Knowledge Base [What placeholders can I use with PRTG?](#)

PRTG Script World

Find useful scripts for custom notifications in the [PRTG Script World](#), written by dedicated PRTG customers around the world and Paessler!

More

 For more information about custom notifications, see the Paessler Knowledge Base, tag-set "[custom-notification](#)".

13.2.8 Mini Probe API

IMPORTANT NOTICE

We do not further develop the Mini Probe API because we plan major changes to the underlying API in PRTG. You can still use the Mini Probe API "as is" but please note that it may be deprecated at any time.

 Knowledge Base: [Where can I find PRTG Mini Probes which are ready to use?](#)

PRTG Mini Probes allow PRTG users to create small probes on any device to meet specific needs. In general, probes are the part of PRTG that run monitoring processes and deliver monitoring results back to the PRTG core server. Mini Probes help gather monitoring data from platforms where it is not possible or is inapplicable to use the common local and remote probes of PRTG. Mini Probes have a less complex implementation than standard probes so that you can create them on any platform. The only requirement is HTTPS connectivity to send monitoring data to your PRTG core server.

Basically, this takes the [Custom Sensors](#)³⁶³⁷ concept to a higher level; you will have a very broad range of possibilities and you can implement amazing functions to get an even better network monitoring experience!

 With the current version of PRTG, you can use the Mini Probe interface with your custom code to implement solutions to special scenarios that you might have in your network. Please note that there are major changes planned to the underlying API in PRTG. Therefore, any code you write now will likely need to be changed later, so it can be used for future versions of PRTG. For example, if the available HTTP Push sensors are not sufficient for your needs, you can still use the Mini Probe API. We will provide further news about changing interfaces as soon as there are more detailed plans available.

 Because the PRTG Mini Probe requires an SSL-secured connection to the PRTG core server, it is not possible by default to connect if SSL is deactivated for PRTG. This is necessary because probably unencrypted passwords will be transferred between probe and core. So it is important to encrypt the connection even on internal routes. If your network setup ensures security in another way (for example, VPN), you can use a registry key option for disabling SSL in order to get a connection to your Mini Probe.

 For more details, see this Knowledge Base article: [How can I disable SSL for Mini Probes?](#)

 The Mini Probe API is not available in PRTG hosted by Paessler.

Here are quick links for ease of use.

- [PRTG Mobile Probe for Android](#)³⁶⁶¹
- [Differences Between Probe Types](#)³⁶⁶¹
- [The PRTG Mobile Probe Protocol](#)³⁶⁶²
- [The PRTG Mini Probe Protocol—Communication and Security](#)³⁶⁶³
- [The PRTG Mini Probe Protocol—Authentication](#)³⁶⁶³

- [The PRTG Mini Probe Protocol—HTTP Requests](#) 
- [Data Format: JSON Definitions](#) 
- [Data Format: JSON Definitions—Sensor Definition](#) 
- [Data Format: JSON Definitions—Tasks Definition](#) 
- [Data Format: JSON Definitions—Data Definition](#) 

PRTG Mobile Probe for Android

Initially we released a mobile probe for Android devices to gather local monitoring data with mobile devices. This mobile probe is a subtype of the Mini Probe. With the PRTG Mobile Probe for Android, you can monitor, for example, wireless LAN (WLAN) coverage, location, battery, HTTP response times, and environmental data such as temperature, pressure, humidity, or light intensity. The available data depends on the available measurement components on the device.

PRTG Mobile Probes for Android usually connect via WLAN and monitor your network from the mobile perspective.

Differences Between Probe Types

The following table shows technical specifications of the two probe types in PRTG.

FUNCTIONALITY	LOCAL AND REMOTE PROBES	PRTG MINI PROBE
Connection Protocol from Probe to Core	Protocol from PRTG	HTTPS
Security	Data is secured with SSL and an access key. New probe connections must be approved by the PRTG administrator. IP and GUID filtering is possible.	The same security level as for local and remote probes.
Estimated Limit for Sensors per Probe	Several thousand sensors	Less than 100 sensors
Estimated Limit for Probes per Installation	Hundreds of probes	Less than 100 probes
Estimated Minimum Scanning Interval	Some seconds	At least 60 seconds

FUNCTIONALITY	LOCAL AND REMOTE PROBES	PRTG MINI PROBE
Estimated Number of Sensor Types	More than 200	A few
Updates to New PRTG Versions by the Core Server	Yes	No
Complexity	High	Very low
Documented API	No	Yes
Supported Platforms	Windows 7 or later (32-bit/64-bit)	Any platform
Scheduling of Sensor Requests Performed by	Probe	Probe
Code Managed by	Paessler AG	Writer of the probe
Probe Supports Pre-Scans for Available Measurements	Yes	No
Sensors Support Inheritance of Settings ¹³⁷	Yes	No
Limitations by Administrator for Allowed Sensor Types that a PRTG User Can Create	Yes	No

The PRTG Mini Probe Protocol

The PRTG Mini Probe Protocol (PMPP) is a simple, lightweight protocol that extends PRTG with custom remote probes. It can be implemented in a variety of programming languages and runs on any kind of platform. These include, for example, Linux, Android, macOS, and iOS.

 PRTG Mini Probes are not intended for high performance monitoring and support only the sensor types that you implement.

The PRTG Mini Probe Protocol—Communication and Security

The PMPP uses GET and POST requests via HTTPS in order to communicate with the PRTG server. All requests are sent to the defined TCP port for the common PRTG web server (default is 443 for SSL), or you specify an extra port explicitly for Mini Probe connections in the [PRTG System Administration—Core & Probes](#)³³⁶³. PRTG Mini Probes use the GET method to receive tasks, and the POST method to send information about the probe and the monitoring results to the PRTG core.

 The data format of some HTTP fields has to be JSON encoded. See [Data Format: JSON Definitions](#)³³⁶³ for data definitions that require JSON. All exchanged data is secured with SSL.

The PRTG Mini Probe Protocol—Authentication

The PMPP uses the same authentication methods as the common PRTG remote probes. The authentication includes the following steps:

- Allow and deny IPs filter
- Deny GIDs filter
- Access key
- Unique GID that must be approved in the PRTG web interface
- In addition, Mini Probes must be allowed to connect in the PRTG Probe connection settings! Additionally, you have to provide the Mini Probe's IP in the **Allow IPs** field (or enter any).

There are no sessions on the server: Every request must contain the required authentication information.

 For more details, see section [System Administration—Core and Probes](#)³³⁶³.

The PRTG Mini Probe Protocol—HTTP Requests

The PMPP includes three different HTTP requests that are sent to the PRTG web server:

- **announce**: An announce request is sent once when the probe starts. Afterwards, the task and data commands are run in a scheduled manner.
- **tasks**: With a tasks request, the probe requests a list of tasks to perform.
- **data**: The data request sends the monitoring results to the core.

All requests of the Mini Probe to the PRTG server must contain the following HTTP fields:

- **gid**: The unique GID of the probe. We recommend a GUID that is generated by the operating system. This identifier must stay the same for as long as the probe installation exists. You can use any string. If you clone a probe, you have to update this field to a new value.
- **key**: An access key as defined in the probe settings of the PRTG server. The key has to be encoded in SHA1 hash (for example, **key=a94a8fe5ccb19ba61c4c0873d391e987982fbbd3**).

- **protocol:** The version of the protocol you use. Currently, this value is "1"

All requests return common HTTP response codes.

 For more information, see section [HTTP API](#)³⁶⁰⁷.

Announce Request

The announce request uses the POST method and provides all required information about the capabilities of the Mini Probe for the PRTG core. The target URL is **https://<yourPRTGserver>/probe/announce**

 This HTTP request must be sent at least once to be able to add sensors. We recommend sending this request every time the probe starts. You should NOT send it with every scanning interval!

The announce request must contain the following HTTP fields:

- **name:** The name of the Mini Probe. PRTG uses this name to create a corresponding node in the device tree.
- **version:** The version number of the Mini Probe you have implemented. This is a single integer number, for example, "1".
- **baseinterval:** The number of seconds between two calls of the task/data requests. We recommend 60 or 300 seconds; depending on the usage, higher or lower values are possible.
- **sensors:** The definition of supported sensors in JSON format.
 See [Data Format: JSON Definitions—Sensor Definition](#)³⁶⁶⁵ for more information.
- **icon** (optional): You can optionally send the file name of a device icon to show it for the mini probe device in the PRTG web interface.
 For details, see our Knowledge Base article [How can I add my own device icons for use in the PRTG web interface?](#)

 If you change the definition of a sensor that has already been announced, these changes will only be active after the next start of PRTG. An existing definition never changes while PRTG is running. However, there is one exception: Setting the "deprecated" flag works without any restart. Because of this, you can replace an existing sensor with a new one that uses another definition.

Tasks Request

The tasks request uses the GET method and is sent from your Mini Probe in the defined scheduler interval to the PRTG core server (for example, every 5 minutes). The target URL is

```
https://<PRTGserver>/probe/tasks
```

This HTTP request returns a list of tasks in JSON format that have to be run by the Mini Probe.

 See [Tasks Definition](#)³⁶⁷² for more information.

Data Request

The data request uses the POST method and contains the HTTP field data. This HTTP field contains any number of sensor results in JSON format. The target URL is

```
https://<PRTGserver>/probe/data
```

You can split the results of one tasks list into several result requests (for example, if some sensors are faster than others). The Mini Probe should combine as many results as possible into one request but keep the time between measurement and reporting of the value at a low level.

See [Data Definition](#) ³⁶⁷³ for more information.

Data Format: JSON Definitions

All data definitions of sensors, tasks, and result data of PRTG Mini Probes are JSON encoded. JSON is a language-independent data format that is used to transmit data objects consisting of attribute-value pairs between a server and an application. Refer to the JSON documentation for a general overview of this data format.

Data Format: JSON Definitions—Sensor Definition

This section shows how you can define the available sensor types for your Mini Probe. Sensor definitions are given in the HTTP field "sensors" of the announce request.

Basic Structure

The sensor types definition is a JSON array where each sensor type is defined in one array element as a JSON object. A JSON object denoting a sensor definition consists of the following JSON name/value pairs:

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
kind	X	Unique identifier for the sensor type in the Mini Probe. Used in the tasks definition to identify the sensor type.  Underscore "_" is not allowed here.	Any string
name	X	The display name of the sensor.	Any string
deprecated	—	You can flag the sensor to status deprecated. A flagged sensor can still run but this kind of sensor will not be shown when you add new sensors to the probe.	1 (= deprecated) 0 (= not deprecated)

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
description	—	A short description of the sensor that is shown in the Add Sensor ³²⁷¹ dialog in the PRTG web interface.	Any string
help	—	A help text that is shown in a popup in the Add Sensor ³²⁷¹ dialog in the PRTG web interface.	Any string
tag	—	A default tag for the sensor that will automatically be added to the sensor.	Any string
default	—	A sensor of this type will automatically be created with the probe if set to "default".	(= set to default) 0 (= not default)
groups	—	In the "groups" array, available settings for this sensor type are defined.	An array of grouped settings JSON objects.  See Definition of Setting Groups Objects ³⁶⁶⁶ for more information.

Definition of Setting Groups Object s

One settings group definition (one element of the "groups" array) consists of three elements:

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
name	X	The internal name of the settings group.	Any unique string

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
caption	X	The label of the settings group as shown in the PRTG web interface.	Any string
fields	X	The available settings of the settings group.	An array of field definition objects. ⓘ See Parameters for Setting Fields for more information.

Parameters for Setting Fields

The following table shows available JSON name/value pairs for setting fields:

NAME	MANDATORY	DESCRIPTION	AVAILABLE IN TYPE	POSSIBLE VALUE
type	X	Type of the field. This defines the possible content.	All	Edit Password Integer Radio ⓘ See Definition of Setting Fields: Field Types for more information.
name	X	The internal name of the field. The name has to be unique per sensor. It is sent with the settings of the probe in the task request.	All	Any unique string

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
 8 Mini Probe API

NAME	MANDATORY	DESCRIPTION	AVAILABLE IN TYPE	POSSIBLE VALUE
caption	X	The label of the field. It is displayed left of the field.	All	Any string
required	—	If a field is defined as required, this field has to be set when adding or editing the sensor settings. Default is not required.	All	0 (= not required) 1 (= required)
default	—	The default value of the field.	All	Any string or integer (depending on the field type)
help	—	A help text that is displayed right of the field.  You can use limited BBCode: "[b]" and "[/b]" for bold, "[i]" and "[/i]" for italics, and "[br]" for linebreak.	All	Any string
maximum	—	The maximum value that is allowed for this field.	Integer	Integer
minimum	—	The minimum value that is allowed for this field.	Integer	Integer

NAME	MANDATORY	DESCRIPTION	AVAILABLE IN TYPE	POSSIBLE VALUE
options	—	A JSON array that provides several radio buttons to choose a desired option.	Radio	"name":"value" pairs. See Example below.

Example

"name":"value" pairs that define radio button options:

```
{
  "1": "This is option 1",
  "2": "This is option 2",
  "XYZ": "Another option"
}
```

Definition of Setting Fields: Field Types

A sensor type can have any number of setting fields that are organized in groups of settings. One field is one element in the "fields" array of a settings group. Currently, PRTG Mini Probes support four different field types for settings:

- **edit**: One line edit field.
- **password**: An edit field with masked characters.
- **integer**: A number field with optional minimum/maximum selection.
- **radio**: A selection of multiple options with radio buttons.

Example

The following is a detailed example that shows the JSON object definition of a sensor type that is used in the HTTP field sensors of the announce request.

This sensor type is called **Sample Sensor** and is from the type **Sample**. It has a description, a help text, and a default tag. There are two setting groups, **Group** and **group2**, with several setting fields (six in the first group, one in the second group). The example also shows how you can use the available JSON name/value pairs in the **fields** array object.

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
8 Mini Probe API

```
[
  {
    "kind": "Sample",
    "name": "Sample Sensor",
    "description": "This is a sample demo sensor",
    "help": "This is the help text of the demo sensors",
    "tag": "demosensor",
    "groups": [
      {
        "name": "Group",
        "caption": "Group",
        "fields": [
          {
            "type": "edit",
            "name": "simpleedit",
            "caption": "Edit Field",
          },
          {
            "type": "edit",
            "name": "extendededit",
            "caption": "Edit Field 2",
            "required": "yes",
            "default": "Default Value",
            "help": "Help text displayed to the right of the field"
          },
          {
            "type": "integer",
            "name": "simplenumber",
            "caption": "Number",
          },
          {
            "type": "integer",
            "name": "number2",
            "caption": "Number 2",
            "required": "1",
            "minimum": 23,
            "maximum": 99,
            "help": "Number field with limit 23-99"
          }
        ]
      }
    ]
  }
]
```

```
    },
    {
      "type": "password",
      "name": "password",
      "caption": "Password",
      "help": "This is a password field"
    },
    {
      "type": "radio",
      "name": "radiotest",
      "caption": "Radio test",
      "help": "This is a radio selection field",
      "options": {
        "1": "This is option 1",
        "2": "This is option 2",
        "3": "This is option 3"
      },
      "default": "2"
    },
  ],
  {
    "name": "group2",
    "caption": "Group 2",
    "fields": [
      {
        "name": "testfield2",
        "caption": "Test2",
        "type": "edit"
      }
    ]
  }
]
]
```

Data Format: JSON Definitions—Tasks Definition

A tasks definition is a JSON array where each task is one object. Tasks contain all name/value pairs as defined in the sensor settings definition, which are filled with the values you have provided. Additionally, the following information is included:

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
kind	X	The type of the sensor.	String
sensorid	X	The ID of the sensor.	Integer
host	X	The IP address/DNS name of the parent device as specified for this device. For the probe device, it is 127.0.0.1 by default.	IP/DNS name
all defined fields	X	All fields that are defined in the sensor setting group objects are included in the tasks definition as name/value pairs.	name/value pairs

 This data comes from PRTG, so the mandatory JSON objects are included automatically.

Example

Definition of two tasks, the first one is the simplest possible one without any values, and the second one uses the sensor settings objects as defined above:

```
[
  {
    "sensorid": "2009",
    "kind": "ping",
    "host": "www.google.com"
  }
  {
    "sensorid": "2010",
    "kind": "sample",
    "host": "www.paessler.com",
    "simpleedit": "Test2",
    "extendededit": "Extended Test",
    "simplenumber": "3",
    "number2": "42",
    "password": "masked text",
    "radiotest": "1",
    "testfield2": "This is test 3"
  }
]
```

Data Format: JSON Definitions—Data Definition

A data definition is a JSON array where each result of a task is one object. Every array element contains the following name/value pairs:

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
sensorid	X	The ID of a specific sensor.	Integer

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
time	—	<p>The time of measurement in UTC/ GMT timezone as JSON number in Unix time format (in milliseconds since Unix epoch, which is 00:00:00 UTC on January 1, 1970). Time values must be strictly chronological, so the Unix time of each measurement must be greater than the one before. The time values should be close to the current time (which is now) to prevent gray sensors.</p> <p> If no time value is provided, the current time (now) is used.</p>	JSON number defining Unix time
message	—	An optional text message.	Any string
channel	X	The channel result values.	<p>An array of name/ value pairs.</p> <p> See Parameters for Data Definitions: Channel Result Values ³⁶⁷⁵ for more information.</p>

 **Examples**

Data definition object with sensor status **OK**:

```
[
  {
    "sensorid": "2003",
    "message": "Optional Message",
    "channel": [
      {
        "name": "Time",
        "mode": "integer",
        "unit": "TimeResponse",
        "value": 6
        "showchart": 1
        "showtable": 1
      }
      {
        "name": "Pages",
        "mode": "counter",
        "unit": "Custom",
        "customunit": "Pages",
        "value": 99
      }
    ]
  }
]
```

Data definition object with sensor status error:

```
[
  {
    "sensorid": "2003",
    "error": "Response",
    "code": 10,
    "message": "Error Message"
  }
]
```

Parameters for Data Definitions: Channel Result Values

The following table shows name/value pairs that can be used in the "channel" array objects of data definition objects:

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
 8 Mini Probe API

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
Name	X	The name of the channel as displayed in user interfaces.	Any string
Value	X	Any number without quotation marks.	An integer, float, or counter value
Mode	—	The type of the value.  Make sure that it matches the provided value, otherwise PRTG will show 0 values.	Integer, float, or counter
Unit	—	The unit of the value.  Setting the correct unit type instead of custom units helps PRTG display received values in a better way.	BytesBandwidth BytesMemory BytesDisk BytesFile TimeResponse TimeSeconds TimeHours Temperature Percent Count CPU: This is a % unit that is accounted to the CPU load in index graphs. Custom (define the name of the unit using the additional field customunit)
ShowChart	—	Init value for the Show in Graphs option.	0 (= do not show graph) 1 (= show graph)

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
ShowTable	—	<p>i The values defined with this element will be considered only on the first sensor scan when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings^[3160].</p> <p>Init value for the Show in Tables option.</p>	<p>0 (= do not show table)</p> <p>1 (= show table)</p>
SpeedSize VolumeSize	—	<p>i The values defined with this element will be considered only on the first sensor scan when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings^[3160].</p> <p>Size used for the display value. For example, if you have a value of 50000 and use Kilo as size, the display is 50 kilo #. Default is One (value used as returned).</p> <p>i For the Bytes and Speed units, this is overridden by the setting in the user interface.</p>	<p>One</p> <p>Kilo</p> <p>Mega</p> <p>Giga</p> <p>Tera</p> <p>Byte</p> <p>KiloByte</p> <p>MegaByte</p> <p>GigaByte</p> <p>TeraByte</p>

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
8 Mini Probe API

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
			Bit KiloBit MegaBit GigaBit TeraBit
SpeedTime	—	See above, used when displaying the speed. Default is Second.	Second Minute Hour Day
decimalMode	—	Init value for the Decimal Places option. If 0 is used in the float mode (use integer), the default is Automatic; otherwise (for float) default is All. ⓘ You can change this initial setting later in the sensor's channel settings ³¹⁶⁰ .	Automatic All Custom
decimalDigits	—	If you define Custom as decimalMode, specify the number of digits after the delimiter.	Integer
ValueLookup	—	Define if you want to use a lookup file (for example, to view integer values as status texts). Enter the ID of the lookup file you want to use, or omit this element to not use lookups.	Any string

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
LimitMaxError	—	<p> See section Define Lookups  for more information.</p> <p> This setting will be considered only on the first sensor scan, when the channel is newly created; it is ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p> <p>Define an upper error limit for the channel. If enabled, the sensor will be set to a "Down" status if this value is overrun and the LimitMode is activated.</p> <p> Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section. While a sensor shows a "Down" status triggered by a limit, it will still receive data in its channels.</p>	Integer

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
LimitMaxWarning	—	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p> <p>Define an upper warning limit for the channel. If enabled, the sensor will be set to a "Warning" status if this value is overrun and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section.</p> <p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p>	Integer

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
LimitMinWarning	—	<p>Define a lower warning limit for the channel. If enabled, the sensor will be set to a "Warning" status if this value is undercut and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section.</p> <p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings.</p>	Integer
LimitMinError	—	<p>Define a lower error limit for the channel. If enabled, the sensor will be set to a "Down" status if this value is undercut and the LimitMode is activated.</p> <p>i Provide the limit value in the unit of the base data type, just as used in the <Value> element of this section.</p>	Integer

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
 8 Mini Probe API

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
		<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p>	
LimitErrorMsg	—	<p>Define an additional message. It will be added to the sensor's message when entering a "Down" status that is triggered by a limit.</p> <p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings³¹⁶⁰.</p>	Any string
LimitWarningMsg	—	<p>Define an additional message. It will be added to the sensor's message when entering a "Warning" status that is triggered by a limit.</p>	Any string

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
LimitMode	—	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings <small>[3160]</small>.</p> <p>Define if the limit settings defined above will be active. Default is 0 (no; limits inactive). If 0 is used, the limits will be written to the sensor channel settings as predefined values, but limits will be disabled.</p>	<p>0 (= no) 1 (= yes)</p>
Warning	—	<p>i The values defined with this element will be considered only on the first sensor scan, when the channel is newly created; they are ignored on all further sensor scans (and may be omitted). You can change this initial setting later in the sensor's channel settings <small>[3160]</small>.</p> <p>If enabled for at least one channel, the entire sensor is set to "Warning" status. Default is 0 (no).</p>	<p>0 (= no) 1 (= yes)</p>

Part 13: Advanced Topics | 2 Application Programming Interface (API) Definition
8 Mini Probe API

NAME	MANDATORY	DESCRIPTION	POSSIBLE VALUE
Message	—	Text the sensor returns in the Message field with every scanning interval. There can be one message per sensor, regardless of the number of channels. Default is OK.	Any string
Error	—	The type of error.  The type is not necessarily shown in PRTG.	Data: The monitored device returned a value but the sensor could not process it. Response: The monitored device reported an error. This includes timeouts, HTTP response codes, etc. Exception: Error in sensor handling. Socket: Socket error.
Code	—	The error code that is stored in the database.	Integer

More

Knowledge Base: How can I disable SSL for Mini Probes?

- <https://kb.paessler.com/en/topic/60356>

Knowledge Base: Where can I find PRTG Mini Probes which are ready to use?

- <https://kb.paessler.com/en/topic/61215>

13.3 Filter Rules for xFlow, IPFIX and Packet Sniffer Sensors

You can use filter rules for the **Include Filter**, **Exclude Filter**, and **Channel Definition** fields of [Packet Sniffer](#)³⁶⁸⁵, [xFlow, and IPFIX](#)³⁶⁸⁶ sensors. The filter rules are based on the following format:

```
field[filter]
```

Here are quick links for ease of use.

- [All Sensors](#)³⁶⁸⁵
- [Packet Sniffer Sensors](#)³⁶⁸⁶
- [NetFlow v5 and jFlow v5 Sensors](#)³⁶⁸⁶
- [NetFlow v9 and IPFIX Sensors](#)³⁶⁸⁷
- [sFlow Sensors](#)³⁶⁸⁸
- [Valid Data Formats](#)³⁶⁸⁸
- [Examples](#)³⁶⁸⁸

Valid Fields for All Sensors

FIELD	POSSIBLE FILTER VALUES
IP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁸)
Port	Any number
SourceIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁸)
SourcePort	Any number
DestinationIP	IP address or DNS name (see Valid Data Formats ³⁶⁸⁸)
DestinationPort	Any number
Protocol	TCP, UDP, ICMP, OSPFIGP, any number
TOS	Type Of Service: any number
DSCP	Differentiated Services Code Point: any number

Additional Fields for Packet Sniffer Sensors Only

FIELD	POSSIBLE FILTER VALUES
MAC	Physical address (see Examples <small>(3686)</small>)
SourceMAC	Physical address
DestinationMAC	Physical address
EtherType	IPV4, ARP, RARP, APPLE, AARP, IPV6, IPXold, IPX, any number
VlanPCP	IEEE 802.1Q VLAN Priority Code Point
VlanID	IEEE 802.1Q VLAN Identifier
TrafficClass	IPv6 Traffic Class: corresponds to TOS used with IPv4
FlowLabel	IPv6 Flow Label

Additional Fields for NetFlow v5 and jFlow v5 Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats <small>(3686)</small>)
SourceASI	Any number
DestinationASI	Any number

Additional Fields for NetFlow v9 and IPFIX Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
ASI	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	<p>IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel.</p> <p>Possible values: IP address or DNS name (see Valid Data Formats)</p>
SourceASI	Any number
DestinationASI	Any number
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address
Mask	Mask values represent subnet masks in with a single number (number of contiguous bits).
DestinationMask	Mask values represent subnet masks in with a single number (number of contiguous bits).
NextHop	IP address or DNS name (see Valid Data Formats)
VLAN	VLAN values represent a VLAN identifier (any number)
SourceVLAN	VLAN values represent a VLAN identifier (any number)
DestinationVLAN	VLAN values represent a VLAN identifier (any number)

Additional Fields for sFlow Sensors Only

FIELD	POSSIBLE FILTER VALUES
Interface	Any number
InboundInterface	Any number
OutboundInterface	Any number
SenderIP	IP of the sending device. This is helpful if several devices send flow data on the same port, and you want to divide the traffic of each device into a different sensor channel. Possible values: IP address or DNS name (see Valid Data Formats)
MAC	Physical address
SourceMAC	Physical address
DestinationMAC	Physical address

Valid Data Formats

- IP fields support wildcards (*), range (10-20) and hostmask (/10, /255.255.0.0) syntax, as well as DNS names.
 -  IPv6 wildcards, IPv6 ranges, and IPv6 hostmasks are not supported.
- Number fields support range (80-88) syntax.
- Protocol and EtherType fields support numbers and a list of predefined constants.

 For detailed information on IP ranges, see section [Define IP Ranges](#).

Examples

All of the following filter rules are valid examples:

```
SourceIP[10.0.0.1]
SourceIP[10.*.*.*]
SourceIP[10.0.0.0/10]
DestinationIP[10.0.0.120-130]
DestinationPort[80-88]
Protocol[UDP]
MAC[00-60-50-X0-00-01]
DSCP[46]
```

You can create more complex expressions using parentheses () and the words **and**, **or**, or **and not**. For example, these are valid filter rules:

```
Protocol[TCP] and DestinationIP[10.0.0.1]
```

This filters for all TCP traffic with the destination IP 10.0.0.1.

```
Protocol[TCP] or DestinationIP[10.0.0.1]
```

This filters for all TCP traffic and all traffic with the destination IP 10.0.0.1.

```
Protocol[TCP] and (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

This filters for all TCP traffic with either the destination IP 10.0.0.1 or the source IP range 10.0.0.120-130.

```
Protocol[TCP] and not (DestinationIP[10.0.0.1] or SourceIP[10.0.0.120-130])
```

This filters for all TCP traffic that has not the destination IP 10.0.0.1 and not the source IP range 10.0.0.120-130.

Related Topics

- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#) 
- [Monitoring Bandwidth via Packet Sniffing](#) 
- [Monitoring Bandwidth via Flows](#) 

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

13.4 Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors

When adding [Custom xFlow sensors](#), [Custom IPFIX](#), or [Custom Packet Sniffing sensors](#), you have the option to provide a **Channel Definition**. In this field enter your channel definitions using the following syntax (one entry per channel):

```
#<id>:<Name>
<Rule>
```

Syntax

- The **<id>** needs to be 1 or a higher number and must be unique for the sensor. This means each channel definition must have a unique ID.
 - ❗ The maximum channel ID you can use is 2147483648 (2^{31}). Higher IDs are not supported. We recommend that you use channel IDs like 1, 2, 3, and so on.
- The **<id>** is linked to the historic data.
 - ❗ As soon as you change the ID, you will lose the history for this particular channel that the ID was linked to.
- One rule can span multiple lines.
- The next rule starts with a # as first character in a line.
- The **<name>** is the channel's display name.
- The rules are processed top to bottom (the number does not matter) and the data is accounted to the first match.
- PRTG adds one channel named **Other** automatically. This channel counts all traffic for which you have not defined a channel.
- After the name you can use an optional [**<unit>**] to override the automatic unit, which is based on the source sensors.

The **<Rule>** syntax is identical to the one described in the [Filter Rules for xFlow and Packet Sniffer Sensors](#) section. Because data is accounted to the first match, make sure you start with the most specific rule at the top and get less specific to the bottom.

❗ We recommend that you write the rules list in an external editor first and then paste it into the **Channel Definition** field of the sensor in PRTG. Otherwise, if the rules contain an error, the entries will be removed when you add the rules in case!

⚠ You cannot delete channels of an existing sensor, even if you remove a channel from the channel definition. You also cannot change the display name of channels using the channel definition of custom flow sensors. Renaming is only possible via [channel settings](#).

Example

General example:

```
#5:HTTP
Protocol[TCP] and
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:

```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```

Related Topics

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#) 3685
- [Monitoring Bandwidth via Packet Sniffing](#) 3512
- [Monitoring Bandwidth via Flows](#) 3514

More

Knowledge Base: How can I change the default groups and channels for xFlow and Packet Sniffer sensors?

- <https://kb.paessler.com/en/topic/60203>

13.5 Define IP Ranges

In some setting fields, you can either enter a host name or single IP address, or you can define IP ranges. PRTG follows a common syntax for this. IP ranges are available, for example, for [xFlow and Packet Sniffer sensors](#)^[430] and for [probe connection settings](#)^[389].

 For the supported syntax of the automatic network discovery functionality in PRTG, see section [Auto-Discovery](#)^[285] (**IP Selection Method**).

Available Options

OPTION	DESCRIPTION	SYNTAX	EXAMPLE(S)
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG will resolve it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address.	a.b.c.d/h or a.b.c.d/e.f.g.h	10.0.0.0/255
Range	Enter an IP address range. Replace each of a , b , c , d by either <ul style="list-style-type: none"> ▪ * (asterisk) for any value; corresponds to 0-255 —or— ▪ x-y for any range between 0 and 255. 	a.b.c.d	10.0.0.1-20 or 10.*.0.* or 10.0.0-50.*

13.6 Define Lookups

PRTG uses **lookups** for some sensor types and for some sensors with custom channels. In general, lookups make data more human friendly because they map status values as returned by a device (usually integers) to more informative expressions in words that show you the status of a monitored device as a clear message.

Additionally, lookups can also define the [sensor status](#) that will be shown in correlation with certain status codes, just like [sensor channel limits](#) can define a sensor status, too. For example, for a printer, PRTG can show a sensor in a yellow **Warning** status with channel values, provided by lookups, like "Toner Low" instead of simple status codes, like "1".

You can customize lookups individually and define your own texts that a sensor channel can show. See the section [Customizing Lookups](#) below.

If a channel uses lookups, you can individually define how to control the sensor status, either using the lookup definition or using limits for numerical values returned by the device. For details, see [Sensor Channels Settings](#), section **Alerting and Limits**.

-  Lookups do not change data in the PRTG database, but they merely change the way sensor channels are shown. Any change to lookup definition files will apply to historic data as well as to live data.
-  Some exceptions apply to the [SNMP Custom String Lookup Sensor](#) that basically does an "inverse lookup". It does not map an integer to a text message but looks only for matching strings in the lookup definition and shows a status based on this text value.

 Customizing lookups is not possible on PRTG hosted by Paessler.

Requirement: Channel Unit "Custom"

All sensor channels with enabled **Value Lookup** need to use the channel **Unit "Custom"**. For details, refer to the section [Sensor Channels Settings](#).

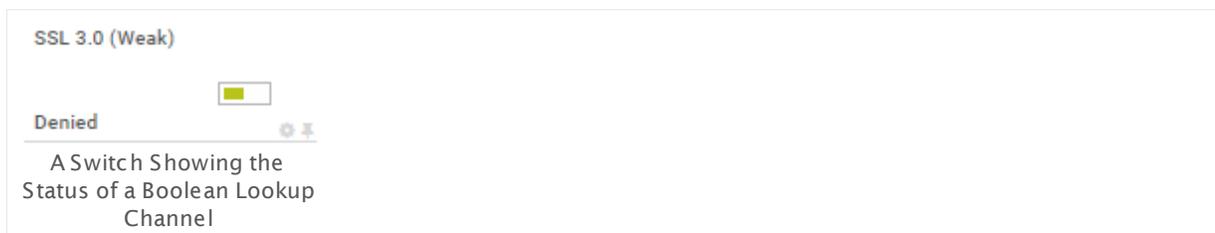
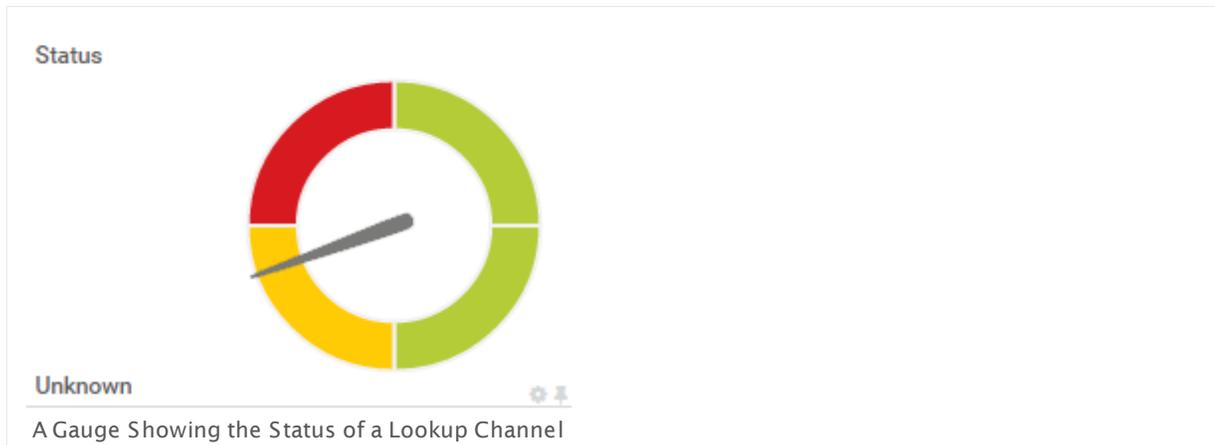
 There are sensors that provide the unit **Value Lookup** for channels in their sensor settings. Do **not** use the "custom" unit for channels of these sensors if you want to use lookups! This would result in malfunctioning lookup channels. For the following sensor types, choose the unit **Value Lookup** in the sensor settings and select your lookup file directly when adding the sensor:

- [Google Analytics Sensor](#)
- [Microsoft SQL v2 Sensor](#)
- [MySQL v2 Sensor](#)
- [Oracle SQL v2 Sensor](#)
- [PostgreSQL Sensor](#)
- [SNMP Custom Advanced Sensor](#)
- [SNMP Custom Table Sensor](#)

Visualization of Lookup Channels

PRTG can display gauges or switches for channels that use lookups. We recommend that you stay below 120 lookup values to display informative gauges for primary channels. Non-primary channels have an upper limit of around 40 lookup values for gauges.

- i** The various states displayed in gauges always follow the clockwise order **Up** (green) < **Warning** (yellow) < **Down** (red) < **Unknown** (gray / black).



Lookups Directory and Format

Lookups are defined in XML format in files ending in `.ovl`. PRTG standard lookup files are located in the [PRTG program directory](#)³⁷³⁴ in the `\lookups` subfolder. These files are maintained by PRTG itself. In each of the files lookups are defined for one or more sensors. Furthermore, the lookups folder contains the `\custom` subfolder to store your customized lookups.

The files follow a basic principle. For each numeric value you can define:

- A message that the sensor will look up and show instead of the numerical value
- The status that the sensor will show

- i** Use the [SNMP Custom String Lookup Sensor](#)¹⁹⁸² to map a string into a corresponding status. Please use the [lookup type](#)³⁷⁰⁰ `SingleInt` for this purpose.

☁ You cannot access this directory on PRTG hosted by Paessler instances.

Example

The following code illustrates the lookup definition for the toner status of the [SNMP HP LaserJet Hardware](#) sensor:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Lookups>
    <SingleInt state="Ok" value="0">Toner Okay</SingleInt>
    <SingleInt state="Warning" value="1">Toner Low</SingleInt>
    <SingleInt state="Error" value="2">No Toner Cartridge Loaded</SingleInt>
  </Lookups>
</ValueLookup>
```

The schema in the example provides an insight how lookups are defined:

- The `<?xml>` tag in the first line defines the content as XML.
- The `<ValueLookup>` tag in the second line contains:
 - The **ID** that is shown in the [Sensor Channels Settings](#).
 - The `desiredValue` attribute contains the value that is used for the calculation of the "Coverage". In this example, **1** is defined as desired value.
 - The `xsi` attributes refer to PRTG's predefined XML schema definitions (which allow easy editing of lookup files with supported editors). We recommend that you use the default value.
- Between the tags `<Lookups>` and `</Lookups>` the particular lookups for the sensor data are defined:
 - A lookup entry starts with a tag containing the type of the status value, the **lookup type** (in this example, this is always `<SingleInt>`).
 - Separated by whitespace, the **state** attribute defines the status the sensor will show. Allowed values are: **Ok**, **Warning**, **Error**, and **None** ("None" does not trigger a status change).
 - The **value** attribute defines which numeric value will trigger the lookup. This is the value that PRTG will receive from the device.
 - The **text** defines the substitution text that is shown instead of the value. For example, this can be a status message.
- The same way all other possible lookups are defined. The lookup definitions are closed by the tag `</Lookups>`. The file closes with `</ValueLookup>`.

In our example, the lookup file will have the following effect:

Value as Reported from HP Printer	Value Shown in PRTG (Sensor Channel)	Sensor Status Shown by PRTG
0	Toner Okay	Up
1	Toner Low	Warning
2	No Toner Cartridge Loaded	Down

The XML Schema

An exemplary schema of the XML files containing the lookup definitions can be sketched like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="..." desiredValue="..." undefinedState="..." xmlns="..." xsi="...">
  <Lookups>
    <SingleInt state="..." value="...">status text</SingleInt>
    <Boolean state="..." value="...">status text</Boolean>
    <BitField state="..." value="...">status text</BitField>
    <Range state="..." from="..." to="...">status text</Range>
    [several other lookup definitions]
  </Lookups>
</ValueLookup>
```

Element	Description	Attributes, Value Assignment, and Content
<code><?xml></code> <code>content</code>	This is the XML declaration. Every XML file begins with it.	<ul style="list-style-type: none"> ▪ version and encoding are "1.0" resp. "UTF-8" ▪ content: <code><ValueLookup>contentValueLookup</ValueLookup></code>
<code><ValueLookup></code> <code>contentValueLookup</code> <code></ValueLookup></code>	Defines the ID of the channel, what desiredValue is used, the status for undefined values (undefinedState), and links to PRTG's predefined schema definitions, which allow editing of lookup files with supported editors.	<ul style="list-style-type: none"> ▪ id: Specifies how the name of the lookup file is shown in the Sensor Channels Settings³¹⁶⁰. ▪ desiredValue³⁶⁹⁹: Please see below. ▪ undefinedState: Optionally define a status for values that are not defined in the lookup file. If the target device returns a value that is not included in the lookup definition, the sensor will show this status (Ok, Warning, Error, or None) with an according message. Without a definition of "undefinedState", the sensor will only show the returned value. ▪ xmlns:xsi/xsi: refers to predefined XML schema definition ▪ contentValueLookup: lookup definitions <code><Lookups>contentLookups</Lookups></code>
<code><Lookups></code> <code>contentLookups</code> <code></Lookups></code>	Defines the particular lookups for the sensor data.	<ul style="list-style-type: none"> ▪ contentLookups: one or more lookup entries, see below
<code><SingleInt></code> <code>status text</code> <code></SingleInt></code>	Each element defines one lookup entry. There can be one or more entries in this format. SingleInt , Boolean , BitField , and Range are lookup types ³⁷⁰⁰ .	<ul style="list-style-type: none"> ▪ state: defines the state the sensor will show; allowed values: Ok, Warning, Error, None
<code><Boolean></code> <code>status text</code> <code></Boolean></code>		<ul style="list-style-type: none"> ▪ value: defines the value that triggers the lookup. Please enter an integer value. <ul style="list-style-type: none"> ⓘ Range needs always both values "from" and "to".
<code><Bit Field></code> <code>status text</code> <code></Bit Field></code>		<ul style="list-style-type: none"> ▪ status text: defines a status text that will be used as substitution text and shown instead the integer value. For example, a status message
<code><Range></code> <code>status text</code> <code></Range></code>		

Because all the XML files containing lookup definitions are delivered in a pre-given schema as indicated above, you can customize lookups accordingly.

Customizing Lookups

If you want to change the status definitions of a specific sensor channel, you basically have to do the following:

- 1) Find out the (file) name of the lookup file in the [settings of the sensor channel](#)³¹⁶⁰ you want to change the behavior for.
- 2) From the [PRTG program directory](#)³⁷³⁴ subfolder `\lookups`, copy this file into the `\lookups\custom` subfolder (ensure you do not change the file name!).
- 3) Change the duplicated file as you like. See the example below.

 This feature is not available in PRTG hosted by Paessler.

All default lookup files are located in the `\lookups` subfolder in the [PRTG program directory](#)³⁷³⁴. To customize existing lookups, copy the desired lookup file from the `lookups` folder to the `\lookups\custom` subfolder or create a new `.ovl` file there. When using the same ID in the `ValueLookup` tag, the files in the `\lookups\custom` folder will have a higher priority than the original files in the `\lookups` folder. This way, PRTG handles your customizations preferably instead of the original lookup settings. If you want to use custom lookup definitions **in addition** to the existing lookups, define a new ID in the lookup file that is not used by another lookup file. PRTG identifies lookup definitions via this ID, it does **not** use the file name.

Open the file with an XML or text editor and adjust the lookups to your personal preferences. You can define your own messages as well as you can customize sensor states for the particular return values. For example, if you do not want show an "Error" (a sensor **Down** status) for the return value "2" but only a warning, then you can replace "Error" with "Warning".

 The possible states are given in the `LookupState.xsd` file in the custom directory. Following the schema of the XML files that are delivered with PRTG enables you to edit the lookups in a safe way.

 If you [imported an oidlib file](#)²²⁴² that contains [lookups](#)³⁶⁹³ (you can see this in section **Lookup** in the MIB Importer), you can define your own sensor states for returning values. If you add an [SNMP Library Sensor](#)²²³⁷ using this oidlib, PRTG will create a lookup definition file using the `lookupname` of the chosen library as `id` parameter. Override this lookup definition with your own custom lookup as described in this section. This is important because lookups that are added via an oidlib will not contain any state definitions and result in a **Warning status**¹⁹⁵¹ of the sensor by default because of the entry `undefinedState="Warning"`.

 If you use an [SNMP Custom String Lookup Sensor](#)¹⁹⁸², you can create a new custom lookup definition in the `\lookups\custom` directory with the expected return values. In this case, use the `lookupname` of the chosen library as `id` parameter to override the lookups from the oidlib file.

 When you save an edited lookup, make sure that it is saved as an `.ovl` file. Otherwise, the lookup might accidentally be saved as a `.txt` file and might not be loaded.

Example for Lookups Customization

For example (just for illustration purposes), imagine you would like

- 1) to have the status "Warning" for all undefined values that the target device might return,
- 2) to change the status for the return value "2" from "Down" to "Warning",
- 3) and to add the status "None" to the [example](#) above.

Then do the following:

- Copy the file `oid.paessler.hplaserjet.tonerstatus` to the `\lookups\custom` subfolder of your PRTG installation.
- Open this file with an editor.
- Leave the ID value unchanged to prioritize the customized lookup to the original file.
- Insert the status definition for undefined values into the ValueLookup element:
undefinedState="Warning"
- Replace "Error" with "Warning" for value "2".
- Add a "SingleInt" element with status "None" for the (hypothetical) return value "3".
- Save the file and [reload](#) the custom lookup folder in PRTG.

The customized lookup file will finally look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1" undefinedState="Warning" xmlns:xsi=
  <Lookups>
    <SingleInt state="Ok" value="0">Toner Okay</SingleInt>
    <SingleInt state="Warning" value="1">Toner Low</SingleInt>
    <SingleInt state="Warning" value="2">No Toner Cartridge Loaded</SingleInt>
    <SingleInt state="None" value="3">Unknown status of toner</SingleInt>
  </Lookups>
</ValueLookup>
```

- See also [SNMP Custom String Lookup Sensor—Example](#) for a lookup definition that maps a string value to a sensor status.

desiredValue Attribute

It is necessary to define a **desiredValue** in the lookup files. The desiredValue corresponds to a status value triggering a lookup. PRTG calculates the percentage of time this specific state has been monitored. The result is displayed for all data tables and graphs that show averaged values.

Considering the example above where the desiredValue is "1", PRTG will calculate the percentage of time the toner status has been "Warning". If in a time span of five minutes four of five sensor scans returned a "Warning" status, PRTG would show an average of 80% for this time span, because in 80% of the time the sensor showed a "Warning".

Lookup Types: SingleInt, Boolean, BitField, Range

Besides the lookup type **SingleInt** as seen above, there are three other lookup types: **Boolean**, **BitField** and **Range**. Using these types you can define lookup values beyond simple integers.

Lookup Type	Description	Syntax
SingleInt	Uses an integer to define a lookup for one status value.	value="int"  The full 32-bit integer range is supported.
Boolean	Uses 0 or 1 to define a lookup for two different status values.	value="0" value="1"
BitField	Uses a bit field for multiple status values.	Only use it if you have basic knowledge about bitmasks. See the section More below for a general introduction.  Every value has to equal a power of two (for example, 1, 2, 4, 8, 16, 32, 64, etc.).  The SNMP Custom String Lookup Sensor does not support BitFields.
Range	Uses an inter range from-to to define a lookup for several status values.	from="int" to="int"  Using ranges, the parameters "from" and "to" always have to be defined. If you want to query only one single value in a range file, this value must be set as parameter for "from" and "to" (for example, from="2" to="2").  The SNMP Custom String Lookup Sensor does not support ranges.  The full 32-bit integer range is supported.

 You can use only **one** kind of lookup type in **one** lookup file. This means, only or **SingleInts**, or **Boolean**, or **BitField**, or **Ranges**. Different lookup types in one file are not allowed.

Define Lookup Files in Sensor Channel Settings

For each sensor with a custom channel, you can define a lookup file to use with the option **Value Lookup** in the [sensor channel settings](#)^[3160]. This option is visible for many **SNMP sensors**, some **application sensors**, and always for the following sensor types:

- [EXE/Script Sensor](#)^[834]
- [EXE/Script Advanced Sensor](#)^[847] (if a **Custom** unit is defined)
- [SNMP Custom Sensor](#)^[1949]

 For details, see section [Sensor Channel Settings](#)^[3160].

Loading Lookups

You can (re)load the defined lookups in the custom folder by clicking the **Load Lookups** button in the PRTG web interface under **Setup | System Administration | Administrative Tools**^[3388].

 A sensor whose lookup file you have modified and reloaded will not re-evaluate this lookup before the next sensor scan. For sensors with large scanning intervals, use the **Scan Now** option from the [context menu](#)^[259] to immediately apply the new lookup definition and to avoid an incorrect sensor status.

Debugging—What will happen if...?

- A return value is defined in the lookups that never will be returned by a device because the value is not assigned: The value will never be triggered, so PRTG simply ignores this entry.
- PRTG receives a return value that is not defined for lookups: No substitution message can be found. PRTG will just show the return value. You can optionally define a status for unknown values with a definition of **undefinedState** in the **ValueLookup** element (see section [Define Lookups—The XML Schema](#)^[3696] above).
- Different lookup types are in one lookup file: This is not allowed and PRTG will discard this lookup definition. If you use miscellaneous lookup types in one file, for example, ranges and singleInts together, the PRTG system will create a ticket when loading lookups or restarting the PRTG server with the following error message: **Value lookup file "[...]" could not be loaded (" " is not a valid integer value)**.
- Incorrect XML code: PRTG will create a new ticket when loading lookups or restarting the PRTG server with a corresponding error message and discard this lookups definition.
- A lookup file has a file ending other than .ovl: The file will not be loaded.
- Alerting is disabled or based on limits: Error and warning states defined in the lookup will not apply. Please ensure you choose the option **Enable alerting based on lookups** in the [channel settings](#)^[3160] if you want to use the lookup definition to control the sensor status.

More

Video Tutorial: How to configure lookups in PRTG Network Monitor

- <https://www.paessler.com/support/videos/prtg-advanced/prtg-lookups>

Wikipedia: Masks (computing)

- http://en.wikipedia.org/wiki/Bit_mask

13.7 Regular Expressions

For some sensors (for example, some [HTTP sensors](#)^[430] and [email sensors](#)^[435]), you can use regular expressions to match a search pattern. PRTG supports **Perl Compatible Regular Expressions (PCRE)**.

⊘ PRTG does not support regex options or regex flags like, for example, `/g` (global), or `/s` (single line), or `/gs`, and will not correctly search for the target string if you try to set options.

See below for examples with the most [common patterns](#)^[3704] and an [example](#)^[3704] for possible matches.

Common Search Patterns

Find matches containing the word **error** or **alarm**:

```
\b(error|alarm)\b
```

Find matches containing the words **error** and **alarm** in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches containing all of the words **t**ree, **f**lower, **l**eam, and **b**ug, in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

ⓘ It is not possible to match an empty string using the PRTG regex search with sensors.

Example

The search pattern

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

will match the following expressions:

- alarm error
- error alarm
- I am an error and I evoke an alarm
- I am an alarm and I indicate an error
- An alarm combined with an error indeed!
- An error combined with an alarm, too!

More

Regex101: Test and debug your regular expressions

- <https://regex101.com/>

Regex Tester: Test Regular expressions interactively

- <http://regexpal.com>

Wikipedia: Regular expression

- http://en.wikipedia.org/wiki/Regular_expression

13.8 Calculating Percentiles

PRTG not only monitors your network and informs you in the case of issues that are worth you taking a closer look at in the here and now. PRTG also stores a lot of historic measurement data gathered from your sensors. This means that you have a great base for statistical analysis and evaluation of what is and was happening in your network.

When creating a [Report](#)³²⁵² with PRTG, you get raw data, sums, averages, and percentages of your monitoring data.

Additionally, PRTG also offers percentile calculation. This statistical method puts your data in order, for example, from the lowest value to the highest value, and calculates the percentile you want, optimally informing you about the distribution of your network-relevant data.

 For example, if you request the 95th percentile, you know that 95 percent of the measured data is below a certain value, and thanks to PRTG, you know what this certain value is.

 If applied, for example, to bandwidth, you know what values you are talking about when talking about the 5 percent of unusually high bandwidth consumption and which value your users do not exceed 95 percent of the time. Service providers often use percentiles to offer fairer billing that excludes infrequent usage peaks.

 If you want to know more about the formula that PRTG uses for percentile calculation, see this Knowledge Base article: [What are percentiles and what differences do they make in PRTG reports?](#)

Create a report for several sensors and device groups using the [Report](#)³²⁵² feature or create reports for single sensors using the [Historic Data Reports](#)²⁰⁴.

More

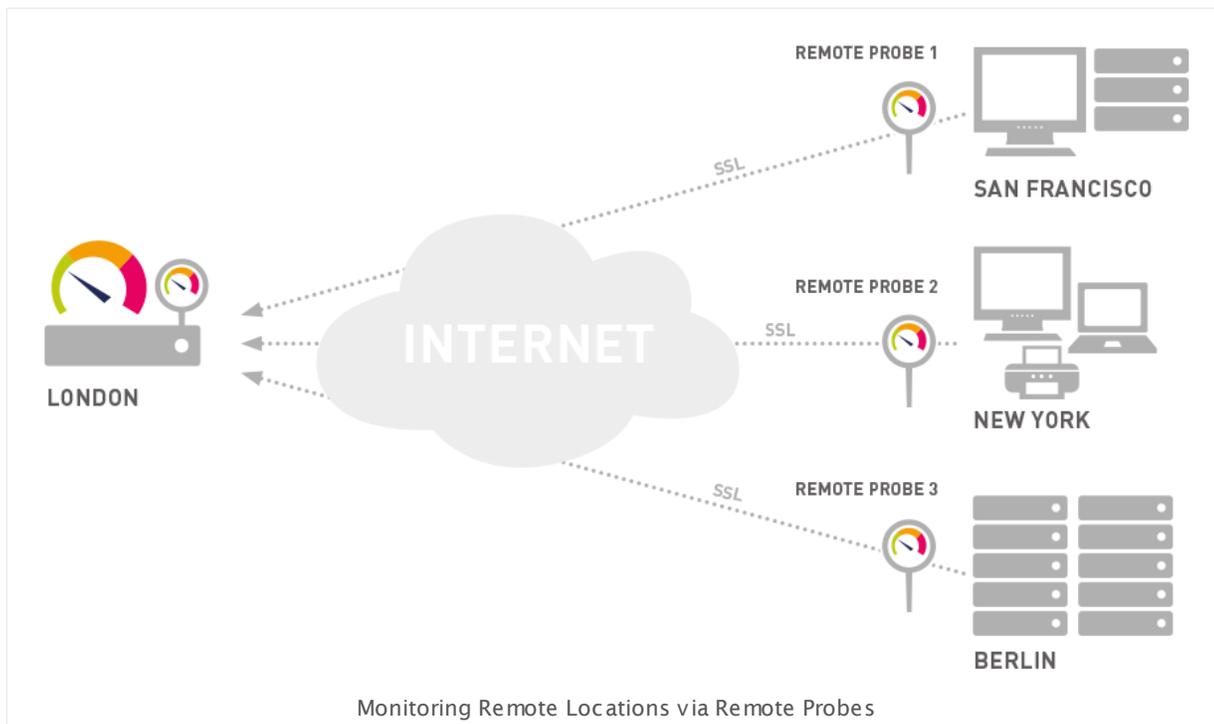
Knowledge Base: What are percentiles and what differences do they make in PRTG reports?

- <https://kb.paessler.com/en/topic/9563>

13.9 Add Remote Probe

* Why are remote probes helpful for monitoring with PRTG? Because you can extend your monitoring.

- Remote probes allow you to monitor different sub-networks that are separated by a firewall from your PRTG on premises core server and to keep an eye on remote locations. You can install [one or more remote probes](#)³⁷⁰⁹.
- Remote probes are useful if you want to distribute monitoring load by taking it from the system running the PRTG core server and putting it on one or more remote probe machines.
- You will need a remote probe if you want to monitor your local network using a PRTG hosted by Paessler instance.
- Remote probes may be suitable monitoring components in several individual scenarios that depend on your custom network setup.



Extend Your Monitoring Now

See the sections linked below for further instructions.

- Background: [Remote Probes and Multiple Probes](#)³⁷⁰⁹
- Installing: [Remote Probe Quick Install](#)³⁷¹³
- Step by Step: [Remote Probe Setup](#)³⁷¹⁹

More

Video Tutorial: Core Server and Remote Probes

- https://www.paessler.com/support/video_tutorials/distributed_monitoring

13.9.1 Remote Probes and Multiple Probes

Upon installation, PRTG creates the first probe automatically, the **Local Probe** in PRTG on premises and the **Hosted Probe** in PRTG hosted by Paessler. They run on the same machine as the PRTG core server and monitor all reachable devices, servers, and services from this system, using the sensors you have configured.

Working only with a local probe should suffice for Local Area Network (LAN) monitoring with PRTG on premises and if you want to monitor one location only. For LAN monitoring with PRTG hosted by Paessler, at least one remote probe is required because the hosted probe can only reach targets that are publicly available via the internet.

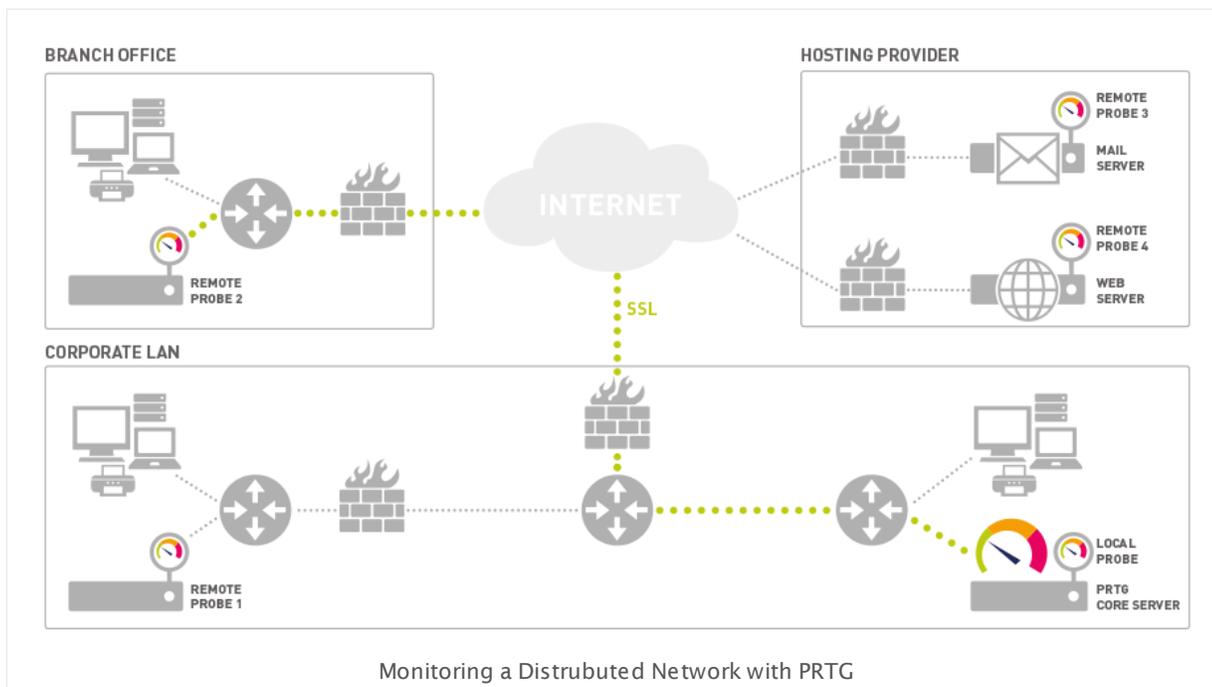
Scenarios Requiring Remote Probes

There are several situations that make it necessary to work with **Remote Probes** in the same LAN or in remote locations. Among these situations are the following:

- You run a PRTG hosted by Paessler instance and want to monitor your local network.
- You have more than one location and you need to make sure that services are available from all locations.
- Your network is separated in several LANs by firewalls, and the local probe cannot monitor specific services across the firewalls.
- You want to monitor systems in a secure network, and you need a secure connection between the PRTG server and this network.
- You want to sniff packets on another computer.
- You want to monitor NetFlow data on another computer.
- You experience performance issues with CPU intensive sensors like packet sniffer or NetFlow sensors and need to distribute the load over more than one PC.

The following chart shows an example for a remote probe scenario.

Part 13: Advanced Topics | 9 Add Remote Probe
1 Remote Probes and Multiple Probes



The PRTG core server inside the **Corporate LAN** (bottom right) is able to monitor:

- Services inside the **Corporate LAN** using the **Local Probe**.
- Services behind a firewall in the **Corporate LAN** using **Remote Probe 1**.
- Secured services inside the **Branch Office** (top left) using **Remote Probe 2**.
- Secured services on **Mail Server** and **Web Server** using **Remote Probe 3** and **Remote Probe 4** installed directly on these servers.
- Public services on the internet using any of the probes.

How Probes Work

As soon as a probe is started, it automatically connects to the [PRTG core server](#)¹²⁶, downloads the sensor configuration, and begins its monitoring tasks. The core server sends new configuration data to a probe as soon as the monitoring configuration is changed by the user. Probes monitor autonomously and send the monitoring results back to the core server for each check they have performed.

If the connections between core and probe fail for any reason (for example, a reboot of the computer running the core server) the probe continues monitoring and stores the results. During a connection loss a buffer stores a maximum of 500,000 sensor results in the RAM memory of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with one minute interval the monitoring results of up to 3 days can be buffered (or 52 minutes for 10,000 sensors with one minute interval). The probe automatically reconnects to the core as soon as it is available again and transmits all monitoring results gathered during the connection loss.

The connection between probe and core is initiated by the probe, secured using Transport Layer Security (TLS). This means that the data sent back and forth between core and probe is not visible to someone capturing data packets. The core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time, the administrator will receive a ToDo [ticket](#)^[230] and will then see the new probe in the device tree.

As a security precaution, the probe must be manually acknowledged by the administrator in the device tree before any sensors can be created and monitored. The administrator can also deny a probe, which will then be disconnected. No further connection attempts will be accepted and the probe IP is added to the **Deny IPs** list in the probes system settings (see [System Administration—Core & Probes](#)^[338] section). This ensures that unauthorized probes cannot connect to a core server.

Because the probe initiates the connection, you must ensure that a connection can be established from the outside world to your core server. For example, you may need to open any necessary ports in your firewall and you may need to specify a Network Address Translation (NAT) rule for your network. The process is the same as if you wanted to allow access to the web server provided by the PRTG core server via port 443, for example. Make sure that you have the TCP port **23560** open or forwarded on both your PRTG core server side and probe side.

If you run PRTG in a cluster installation, remote probes also connect to your failover node(s) in addition to the master node and send monitoring data. This works as described above for a single PRTG server. If your master node fails, you can still see monitoring data on your failover (s). You can define the **Cluster Connectivity** of each probe in its [Administrative Probe Settings](#)^[371].

Automatic Probe Update

Whenever a new version of PRTG is installed on the core server, all remote probes will automatically download and install the updated version of the probe as soon as they reconnect to the updated core installation.

The local probe has already been updated during the core installation. All remote probes automatically download the new binaries using the TLS-secured probe or core connection. The download of the 4 MB file takes anywhere from a few seconds (in a LAN) to a few minutes (via internet connections), depending on the available bandwidth. As soon as the update has been downloaded the probe disconnects, installs the update, and reconnects to the core server. This takes between 20 and 100 seconds. Please note that during the update phase the monitoring of the local probe can be affected due to the bandwidth required for the downloads.

i If the automatic update of a remote probe fails for some reason, please update the remote probe manually by [downloading and executing the installer](#)^[371] on the probe computer. If a remote probe keeps being disconnected after an update, please check if the server with the remote probe has two network connections with different IP addresses. Make sure these addresses are in the list of allowed IPs in the [Core & Probes settings](#)^[338].

More

- [Install a PRTG Remote Probe Using Installer](#)^[101]
- [Remote Probe Quick Install](#)^[3713]

Part 13: Advanced Topics | 9 Add Remote Probe
1 Remote Probes and Multiple Probes

Video Tutorial: Core Server and Remote Probes

- https://www.paessler.com/support/video_tutorials/distributed_monitoring

13.9.2 Remote Probe Quick Setup

Install a PRTG Remote Probe directly by right-clicking on a device in the PRTG device tree. This semi-automatic installation mechanism is an alternative to the [Remote Probe Setup Using Installer](#)^[101].

 This is an experimental feature. It may not work in all situations. In this case, please see [Debugging](#)^[3718] and try the [standard remote probe installation](#)^[101].

 This feature is not available in PRTG hosted by Paessler.

 To install a Remote Probe directly from the device tree in the PRTG web interface, follow the steps below.

- [Step 1: Meet the Requirements](#)^[3713]
- [Step 2: Prepare the Core Server](#)^[3714]
- [Step 3: Provide Credentials](#)^[3715]
- [Step 4: Install the Remote Probe](#)^[3716]
- [Step 5: Approve the New Remote Probe](#)^[3717]

Before you start, take a closer look at the requirements in the first three steps.

 Do you run PRTG Network Monitor in a cluster? Then mind this [important note](#)^[3715].

Step 1: Meet the Requirements

 To install a probe remotely on a computer please ensure that the following conditions are true.

- The target computer runs the operating system Windows 7 or later.
- The target computer is accessible through Remote Procedure Call (RPC). This is usually the case when your PRTG server and the target computer are located in the same LAN segment. Otherwise, open Windows `services.msc` on the target computer and start the Remote Procedure Call (RPC) service.
- Programs are allowed to communicate through your Windows Firewall. Open the settings of your Firewall and choose **Allow programs to communicate through Windows Firewall**. Mark the check box for **Remote Service Management**, and the checkbox **Public** in the corresponding line.
- Connections between remote probes and the PRTG core server require port **23560**. Please open or forward this port in your firewall configuration.

 You cannot install a remote probe on the local probe or hosted probe device and the Remote Probe Quick Setup is also not available for devices on remote probes. Please use the [Remote Probe Installer](#)^[3719].

 You cannot install a remote probe on the computer the PRTG core server runs on because the core server already includes a local probe service or hosted probe service respectively.

Step 2: Prepare the Core Server

! Because your remote probe needs to connect to your PRTG core server, PRTG needs to accept incoming remote probe connections. So, on PRTG on premises, prepare your PRTG server first when you want to install the remote probe.

Edit the relevant settings in [System Administration—Core & Probes](#)³³⁶⁸. From the main menu in the [PRTG web interface](#)¹⁶⁸⁸, select **Setup | System Administration | Core & Probes** to access the probes settings and go to the **Probe Connection Settings**.

The screenshot shows the 'System Administration' web interface. The 'Core & Probes' tab is active. Under 'Proxy Configuration', the 'Use Proxy Server' option is set to 'No, use direct connection to the internet (default)'. Under 'Probe Connection Settings', the 'Probe Connection IPs' option is set to 'All IPs available on this computer'. The 'Access Keys' field contains a list of GUIDs. The 'Allow IPs' field is set to 'any'. The 'Deny IPs' and 'Deny GIDs' fields are empty. The 'Mini Probes' option is set to 'Allow Mini Probes to connect to an extra port'. The 'Mini Probe Port' is set to 8090. A 'Save' button is visible next to the 'Probe Connection IPs' options.

System Administration

User Interface Monitoring Notification Delivery **Core & Probes** User Accounts User Groups Administrative Tools

Proxy Configuration

Use Proxy Server No, use direct connection to the internet (default)
 Yes, in our network a proxy is mandatory

Probe Connection Settings

Probe Connection IPs Local Probe only, 127.0.0.1 (PRTG will not be accessible for Remote Probes) All IPs available on this computer Specify IPs **Save**

Access Keys

Allow IPs

Deny IPs

Deny GIDs

Mini Probes No Mini Probes
 Allow Mini Probes to connect to the web server
 Allow Mini Probes to connect to an extra port

Mini Probe Port

Probe Connection Settings in System Administration

Step 1: Probe Connection IPs

By default, a core server accepts connections from the **Local Probe only** (IP address **127.0.0.1**). This setting is the most secure setting, but it does not allow any remote probe to connect to your PRTG core server.

To accept remote probes, choose one of the following settings:

- **All IPs available on this computer:** Any IP on your core server system accepts incoming probe connections.
- **Specify IPs:** Specify selected IP addresses that accept incoming connections.

Step 2: Allow IPs

In the **Allow IPs** field, you can enter the IP address of the computer you want to install a remote probe on. To make things easier, you can also enter the word **any**. Any will set the PRTG core server to accept remote probes connecting from any IP address.

 If you use **any**, make sure you write the word in lower case only! Any other variations will not be valid!

Changing other settings is not required. For details about the fields for **Access Keys**, **Deny IPs**, and **Deny GIDs** see section [System Administration—Core & Probes](#).

When you are done, click **Save** to save your settings.

 If you change this setting, PRTG needs to restart the core server to apply your changes. After clicking the **Save** button, a dialog box appears that asks you to confirm the required core server restart. Click **OK** to trigger the restart and follow the instructions on the screen. During the restart all the users of the PRTG web interface, of the [Enterprise Console](#), or of [PRTG Apps for Mobile Network Monitoring](#) will be disconnected and reconnected.

 To edit the core-probe connection settings you can also use the [PRTG Administration Tool](#) on your core server.

PRTG Cluster and Remote Probes Outside the LAN

 If you use the [Clustering](#) feature of PRTG and you want to run remote probes outside your local network, you have to make sure your cluster nodes and the addresses they use are reachable from the outside! Check your cluster node settings under [System Administration—Cluster](#) before installing a remote probe outside your local network. Enter addresses (DNS names or IPs) that are valid for both cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

 If you already have a remote probe installed outside your LAN and the probe is disconnected because of this, please follow these steps:

1. Uninstall the current remote probe.
2. Update the [cluster node settings](#) with addresses that are reachable from outside your LAN.
3. Restart your PRTG core servers.
4. Install the remote probe again. It will then obtain the IP address or DNS name entries that it can reach.

 See also section [Failover Cluster Configuration—Remote Probes in Cluster](#).

Step 3: Provide Credentials

If not done yet, [add a device](#) to PRTG that represents the target computer on which you want to install the remote probe. Set the correct Windows credentials for this device.

Part 13: Advanced Topics | 9 Add Remote Probe 2 Remote Probe Quick Setup

- Open the [Device Settings](#)^[402].
- In the **Credentials for Windows Systems** section, provide **Domain or Computer Name**, **User**, and **Password** for the target computer.
- You can also [inherit](#)^[137] the credentials from the settings of a parent object in the device tree.

Make sure this user account has administration rights on the target computer.

Step 4: Install the Remote Probe

- In the device tree overview, open the [context menu](#)^[254] of the target device.
- Choose **Device Tools | Install Remote Probe...**
 - ❗ This option is only available on devices on the PRTG on premises local probe.
- The install assistant will appear on a new page.

[Install Remote Probe on Device Workstation \(home\)](#)

Please note: This is an experimental feature, it may not work in all situations. Please send your feedback to support@paessler.com.

You are about to install a PRTG Remote Probe on the computer "Workstation (home)". This will allow PRTG to monitor this computer locally instead of using remote monitoring features. This can be a good workaround for performance or authentication problems (for example, for WMI sensors) sometimes. Additionally, this will allow you to use some probe-only sensors like Packet Sniffing, NetFlow, and others.

Details

Device Name	Workstation (home) (wdf)
Status	OK
Priority	★★★★☆
Parent Probe	Local Probe (Local Probe) ...
Parent Group	Local Probe (Local Probe) ...
Sensors by State	(Total: 0)

[Prerequisites](#)

Please make sure you fulfill the following conditions.

- The target device must be a computer with a **supported Windows version**.
- The target computer must be accessible through **RPC** (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- Open or forward **port 23560** in your firewall to allow connections between the probe and your PRTG core server.
- Windows credentials must be set in the **device settings** or its parents' settings (current user name: paesslergmbh\Testadmin) and the user account must have administration rights on the target machine.
- You have to allow remote probe connections to your PRTG core server. Open the **Core & Probes** tab in the System Administration of your PRTG web interface. In section **Probe Connection Settings** choose the option **All IPs available** on this computer or specify IPs for the setting **Probe Connection IPs**. Do not use the "Local Probe only" (127.0.0.1) setting! (Current setting: 172.17.101.192,127.0.0.1)

[Start Probe Installation](#)

The installation will take between 10 and 100 seconds.

[Install Remote Probe on "Workstation \(home\)"](#)

Remote Probe Installation Assistant

The installation assistant is divided into four sections:

- Experimental feature notice and short introduction
- **Details:** Overview about the device: name, status, priority, parent probe, parent group, and sensor states in place with their number
- **Prerequisites:** For details, see [Step 1](#)^[3713].
- **Start Probe Installation:** Time estimation for installation and installation start button

Make sure you meet the following requirements. If not, PRTG cannot start the installation process. Open requirements are highlighted in red.

Prerequisites

Please make sure you fulfill the following conditions.

- The target device must be a computer with a supported Windows version.
- The target computer must be accessible through RPC (this is usually the case when your PRTG server and the target computer are located in the same LAN segment).
- Open or forward port 23560 in your firewall to allow connections between the probe and your PRTG core server.
- You cannot install a remote probe on a probe device.
- Windows credentials must be set in the device settings or its parents' settings (current user name: test\test) and the user account must have administration rights on the target machine.
- **Please correct before proceeding:** You have to allow remote probe connections to your PRTG core server. Open the Core & Probes tab in the System Administration of your PRTG web interface. In section Probe Connection Settings choose the option All IPs available on this computer or specify IPs for the setting Probe Connection IPs. Do not use the "Local Probe only" (127.0.0.1) setting! (Current setting: 127.0.0.1)

Installation Unable to Start because Prerequisites Are Not Met

If everything is okay you can install the remote probe on the target computer by clicking the button **Install Remote Probe on "[device name]"**. Wait until the process has ended.

- ✓ If the installation was successful, the following message will appear in the **Start Probe Installation** section: **Done. Result is: OK.**
- ⓘ Every time you start an installation, PRTG automatically adds a new key to **Access Keys** in [System Administration—Core & Probes](#)³³⁶⁸, no matter if the installation has been successful or not.

Step 5: Approve the New Remote Probe

If the installation was successful, you will receive further instructions after the result message. As indicated, go back to the [device tree](#)¹⁸¹ and acknowledge the new probe. The approval button will appear under the node of the new remote probe. You will also receive a new [ToDo ticket](#)²³⁰.

Click **Approve and auto-discover new probe** to acknowledge the created remote probe and instantly start an [Auto-Discovery](#)²⁸² in this network. Click **Approve new probe** to acknowledge the remote probe without running an auto-discovery. You can also discard the probe by clicking **Deny new probe**.

- ⓘ When denying or removing a remote probe, this device's global ID (GID) will be included into **Deny GIDs** in [System Administration—Core & Probes](#)³³⁶⁸. Future probe connections from this device will be denied automatically.
- ⓘ Denying the remote probe in the PRTG device tree does **not** uninstall the probe, but only denies access to the core server. The probe will continue to run on the target system until you uninstall it manually.

After approving, the approval button will turn into a **Working** status. Please wait while the probe connects. Once approved, PRTG automatically creates a set of sensors for the probe to ensure that bottle-necks on the probe will always be noticed. We recommend that you keep these sensors. Now you can create groups, devices and sensors to customize your monitoring via the new probe.

Debugging

- Please note that installing a remote probe directly from the device tree in the PRTG web interface is an experimental feature. It may be the case that this approach is not possible in all situations.
- Please follow the steps of this chapter closely when encountering problems with the Remote Probe Quick Install. Especially consider the conditions as described in [Step 1](#)³⁷¹³ of this section like Windows Firewall settings.
- If the quick installation procedure described in this section does not work with your setup, please install your remote probes manually and see how to do so in [Remote Probe Setup Using Installer](#)³⁷¹⁹.

More

Knowledge Base: How can I customize PRTG's ports for core-probe-connections?

- <https://kb.paessler.com/en/topic/65084>

13.9.3 Remote Probe Setup Using Installer

In section [Install a PRTG Remote Probe](#)^[101], we accompany your remote probe installation using the [Remote Probe Installer](#).

These are the [Steps to Go](#)^[101]:

1. [Prepare the PRTG Core Server](#)^[102]
2. [Download the Remote Probe Installer](#)^[104]
3. [Install the Remote Probe](#)^[105]
4. [Approve New Probe and Start Monitoring](#)^[107]

Moreover, there is a [Debugging Remote Probe Connection Problems](#)^[109] section in case you are facing issues after the installation.

 For a semi-automatic installation of a Remote Probe directly from the device tree in the PRTG web interface, see section [Remote Probe Quick Setup](#)^[3713].

 Do you run PRTG in a cluster? Then mind this [important note](#)^[103].

More

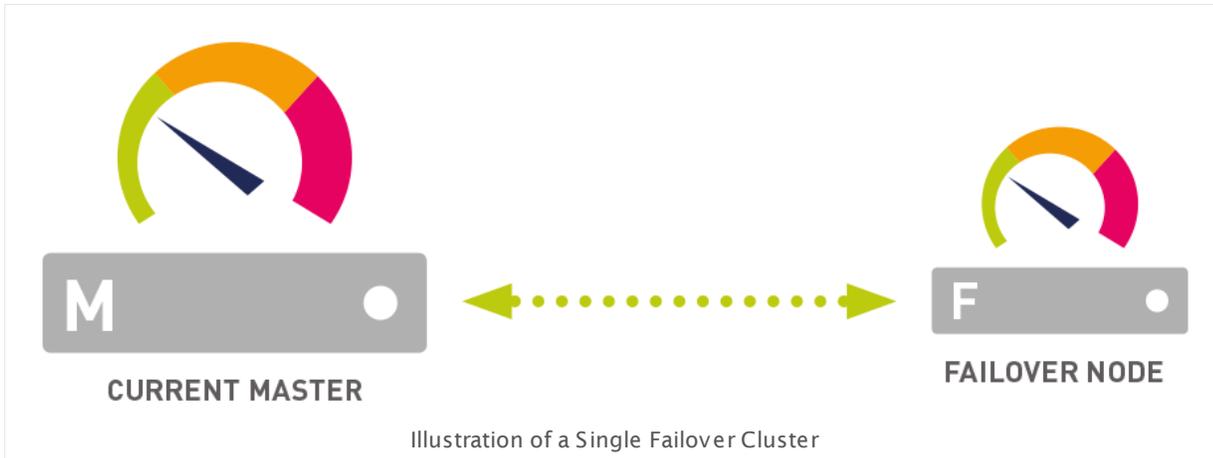
Knowledge Base: How can I customize PRTG's ports for core-probe-connections?

- <https://kb.paessler.com/en/topic/65084>

13.10 Failover Cluster Configuration

PRTG offers single failover clustering in all licenses—even in the freeware edition. A single failover cluster consists of two servers (**Current Master** node and **Failover** node), each of them running one installation of PRTG. They are connected to each other and exchange configuration and monitoring data.

☁ This feature is not available in PRTG hosted by Paessler.

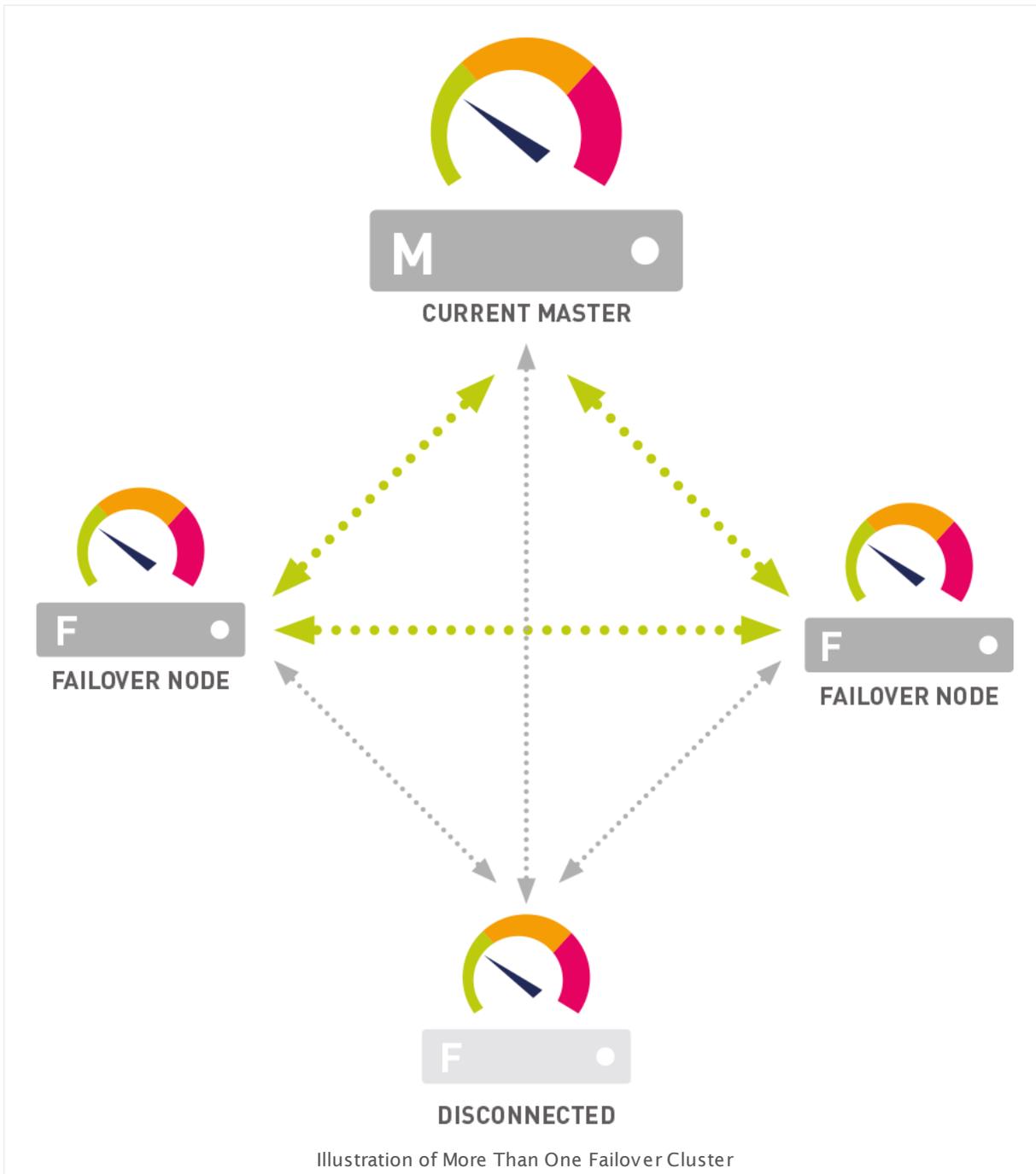


To set up a cluster you need two or more servers. One [PRTG core server installation](#)^[89] is necessary on each of them—with different settings configured for each type of node. In return, you benefit from seamless, highly available monitoring with automatic failover and multi-location monitoring.

In a cluster, you can run:

- **1 Master Node**
On the master node, you set up your devices and configuration. Notifications, reporting, and many other things are also handled by the master node.
- **Up to 4 Failover Nodes**
You can install one, two, three, or four additional nodes for fail-safe, gapless monitoring. For more than one failover node, [you need additional licenses](#)^[3732]. Each of these nodes can monitor the devices in your network independently, collecting their own monitoring data. You can review the data in a summarized way that enables you to compare monitoring data from different nodes.

i During an outage of one node, you will see data gaps for the time of the outage on that node. However, data for that time span will still be available on all other cluster nodes.



Before Getting Started: Cluster Notes

Configuring a cluster with one failover node is the most common way to set up seamless network monitoring with PRTG. You will need two servers that run any Windows version (Windows 7 or later). Your servers can be real hardware (strongly recommended!) or virtual machines.

For details, see section [Detailed System Requirements](#)^[26].

Please consider the following notes about PRTG clustering.

- Your servers must be up and running.
- Your servers must be similar in regard to the system performance and speed (like CPU, RAM memory).
- In a cluster setup, each of the cluster nodes will individually monitor the devices added to the **Cluster Probe**. This means that monitoring load will increase with every cluster node. Please make sure your devices and network can handle these additional requests. Often, a larger scanning interval for your entire monitoring is a good idea. For example, set up a scanning interval of 5 minutes in the [Root Group Settings](#)^[331].
- We recommend that you install PRTG on dedicated real-hardware systems for best performance.
- Please bear in mind that a server running a cluster node may in rare cases be rebooted automatically without notice (for example, because of special software updates).
- Both servers must be visible for each other through the network.
- Communication between the two servers must be possible in **both directions**. Please make sure that no software or hardware firewall blocks communication. All communication between nodes in the cluster is directed through one specific TCP port. You will define it during cluster setup (by default, it is **TCP port 23570**).
- **Email notifications for failover:** The **Failover Master** will send notifications if the **Primary Master** is not connected to the cluster. To ensure that PRTG can deliver emails in this case, please configure the [Notification Delivery](#)^[336] settings so that PRTG can use them to deliver emails from your failover node as well. For example, use the option to set up a secondary Simple Mail Transfer Protocol (SMTP) email server. This fallback server must be available for the failover master so that it can send emails over it independently from the first email server.
- Make your servers safe! From every cluster node, there is full access to all stored credentials as well as other configuration data and the monitoring results of the cluster. Also, PRTG software updates can be deployed through every node. So, please make sure you take security precautions to avoid security attacks like hackers and Trojans. Secure every node server the same careful way as the master node server.
- Run the nodes in your cluster either on 32-bit or 64-bit Windows versions only. Avoid using both 32-bit and 64-bit versions in the same cluster, as this configuration is not supported and may result in an unstable system. Also, ZIP compression for the cluster communication will be disabled and you may encounter higher network traffic between your cluster nodes.
- If you run cluster nodes on Windows systems with different timezone settings and use [Schedules](#)^[338] to pause monitoring of defined sensors, schedules will apply **at the local time of each node**. Because of this, the overall status of a particular sensor will be shown as **Paused** every time the schedule matches a node's local system time. Please use the same timezone setting on each Windows with a cluster node to avoid this behavior.
- The password for the **PRTG System Administrator** login to PRTG is not automatically synchronized on cluster nodes. You need to manually change it on each node. On a failover node, open the [PRTG Administration Tool](#)^[3574] and change the password on the **Administrator** tab. Click **Save&Close** to save your new password.

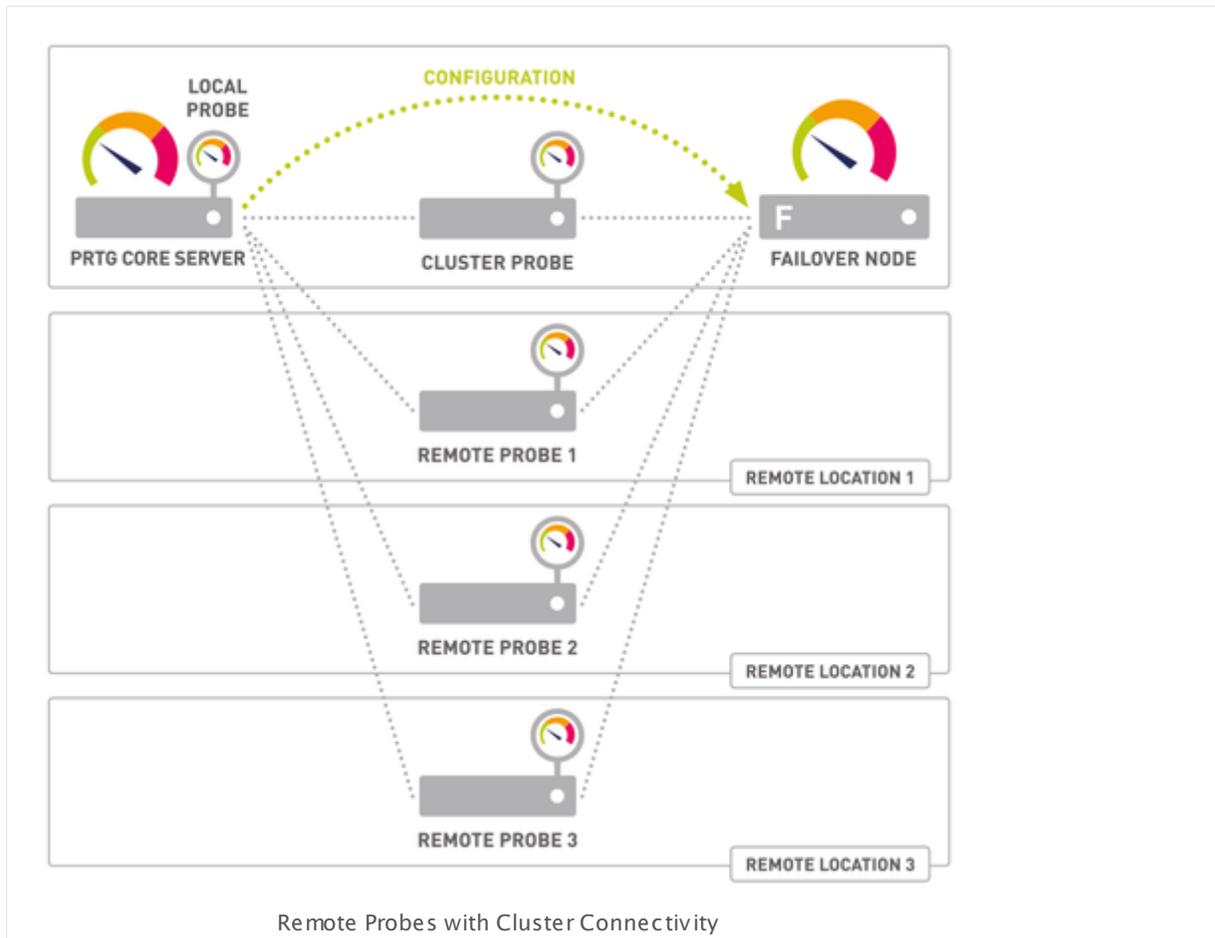
- Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not officially supported. For each additional failover node, divide the number of sensors by two.

In cluster mode, you cannot use sensors that wait for data to be received. Because of this, you can use the following sensor types only on a [local or remote probe](#)¹²⁶:

- [HTTP Push Count](#)¹⁰⁴⁹
- [HTTP Push Data](#)¹⁰⁵⁹
- [HTTP Push Data Advanced](#)¹⁰⁷⁰
- [IPFIX](#)¹¹⁸⁶ and [IPFIX \(Custom\)](#)¹²⁰⁰
- [jFlow V5](#)¹²²³ and [jFlow V5 \(Custom\)](#)¹²³⁷
- [NetFlow V5](#)¹⁴⁰³ and [NetFlow V5 \(Custom\)](#)¹⁴¹⁷
- [NetFlow V9](#)¹⁴³⁰ and [NetFlow V9 \(Custom\)](#)¹⁴⁴⁴
- [Packet Sniffer](#)¹⁴⁹⁴ and [Packet Sniffer \(Custom\)](#)¹⁴⁹⁷
- [sFlow](#)¹⁷⁴⁰ and [sFlow \(Custom\)](#)¹⁷⁵⁴
- [SNMP Trap Receiver](#)²⁴⁷⁹
- [Syslog Receiver](#)²⁶⁵⁶

Remote Probes in Cluster

PRTG provides cluster support for remote probes. This means that all your probes can connect to all your cluster nodes, the primary master node as well as the failover node. Because of this you can still see monitoring data of remote probes and sensor warnings and errors even when your master node fails.



✘ Please consider the following notes about PRTG clustering with remote probes.

- You have to allow remote probe connections to your failover nodes. To do so, log in to each server in your cluster and open the [PRTG Administration Tool!](#)³⁵⁶⁶. On the **Core Server** tab, define to accept connections from remote probes on each cluster node.
- If you use **remote probes outside your local network**: You have to use IP addresses or DNS names for your cluster nodes that are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Open the [System Administration—Cluster](#)³³⁹⁴ settings and adjust the entries for cluster nodes accordingly so that these addresses are reachable from the outside. New remote probes try to connect to these addresses but cannot reach cluster nodes that use private addresses.
- If you use Network Address Translation (NAT) with **remote probes outside this NAT**: You have to use IP addresses or DNS names for your cluster nodes that are reachable from the outside. If your cluster nodes are inside the NAT and the cluster configuration only contains internal addresses, your remote probes from outside the NAT will not be able to connect. The PRTG core server must be reachable under the same address for both other cluster nodes and remote probes.
- A remote probe only connects to the PRTG core server with the defined IP address when starting. This PRTG server must be the **Primary Master!**

- Initially, existing remote probes are not visible on failover nodes. You need to set their **Cluster Connectivity** first in the [Administrative Probe Settings](#)³⁷¹ to be visible and working with all cluster nodes. Choose option **Probe sends data to all cluster nodes** for each remote probe that you want to connect to all cluster nodes.
- Newly connected remote probes are visible and working with all cluster nodes immediately after you have acknowledged the probe connection. The connectivity setting **Probe sends data to all cluster nodes** is default for new probes.
- As soon as a probe is activated for all cluster nodes, it connects automatically to the correct IP addresses and ports of all cluster nodes.
- Once a remote probe has connection data from the Primary Master, it can connect to all remaining cluster nodes also when the Primary Master fails.
- Changes to connection settings of cluster nodes are automatically sent to your remote probes.
- If a PRTG server (which is a cluster node) in your cluster is currently not running, your probes will [deliver monitoring data](#)³⁷¹⁰ after the restart of this server. This happens individually for each PRTG server in your cluster.
- If you switch on cluster connectivity for a probe, it will not deliver monitoring data from the past when cluster connectivity was off. For sensors using difference values, the difference between the current value and the last value is shown with the first new measurement (if the respective sensor previously sent values to the PRTG server).
- Except for this special case, all PRTG servers show the same values of sensors on devices you add to the Cluster Probe.
- The responsible PRTG server for the configuration and management of a remote probe is always the master that is currently active. This means that all tasks of the PRTG core server are only executed by the current master. If you use a split cluster with several master nodes, only the master that appears first in the cluster configuration is responsible.

i You can use remote probes in a cluster as described above, which is showing monitoring data of all your probes on all nodes in your cluster. However, you cannot cluster a remote probe itself. To ensure gapless monitoring for a specific remote probe, install a second remote probe on a machine in your network next to the existing probe, and create all devices and sensors of the original probe on it. For example, you can [clone](#)³¹⁹³ the devices from the original probe. The second probe would be a copy of the first probe then and you can still monitor the desired devices if the original probe fails.

i Probes that send data to all cluster nodes result in increased bandwidth usage. Choose the option **Probe sends data only to primary master node** in the [Administrative Probe Settings](#)³⁷¹ for one or more remote probes to lower bandwidth usage if necessary.

i Please explicitly check on each cluster node if a remote probe is connected. PRTG does not notify you if a remote probe is disconnected from a node in the cluster. For example, log in to the PRTG web interface on a cluster node and check in the device tree if your remote probes are connected.

Start Now!

Ready to get started? Go to section [Failover Cluster Step by Step](#)³⁷²⁷!

More

Knowledge Base: What's the Clustering Feature in PRTG?

- <https://kb.paessler.com/en/topic/6403>

Knowledge Base: What are the bandwidth requirements for running a PRTG Cluster?

- <https://kb.paessler.com/en/topic/8223>

Knowledge Base: What is a Failover Master and how does it behave?

- <https://kb.paessler.com/en/topic/7663>

Knowledge Base: I need help with my PRTG cluster configuration. Where do I find step-by-step instructions?

- <https://kb.paessler.com/en/topic/41913>

Knowledge Base: PRTG Cluster: How do I convert a (temporary) Failover Master node to be the Primary Master node?

- <https://kb.paessler.com/en/topic/34853>

Paessler Blog: Cluster Support for Remote Probes: Failover Nodes Show Remote Probe Data

- <https://www.paessler.com/blog/2015/07/02/all-about-prtg/cluster-support-for-remote-probes>

13.10.1 Failover Cluster Step by Step

This section will guide you through a step-by-step process to set up a failover cluster. Please follow these instructions carefully to successfully integrate two or more PRTG installations into one failover cluster.

 Before getting started, please make sure you consider the information in section [Failover Cluster Configuration](#)³⁷²⁰.

 This feature is not available in PRTG hosted by Paessler.

Step 1: Install Core Servers

We will start with setting up a single failover cluster, consisting of two PRTG core server installations, each running on an individual server. Please use your license key twice to install the PRTG core server on two different computers.

If you already run an installation of PRTG, this will be your future Master Node. In this case, please install a second core server on another computer only. Make sure you use the same license key for both installations.

Before you start to set up a cluster, please make sure you run exactly the same PRTG version (build number) on all (future) nodes (install updates for existing installations, if necessary).

 Once the cluster is established, any updates you install on one node will be deployed to all other cluster nodes automatically.

 For details about the installation process, see [Install a PRTG Core Server](#)⁸⁹¹.

Step 2: Configure Master Node

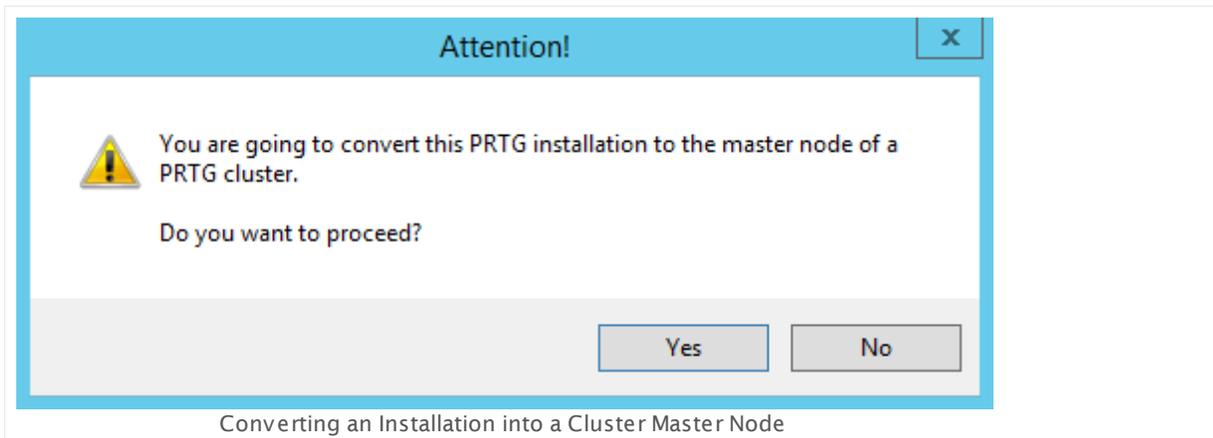
Decide which of your PRTG core server installations will be your future Master Node. If you already run an installation of PRTG in your network for some time, this should be your master, so your existing monitoring configuration is being kept.

On the Master Node server, from the Windows start menu, open the [PRTG Administration Tool](#)³⁵⁶⁸. On the Cluster tab, click on the following button:

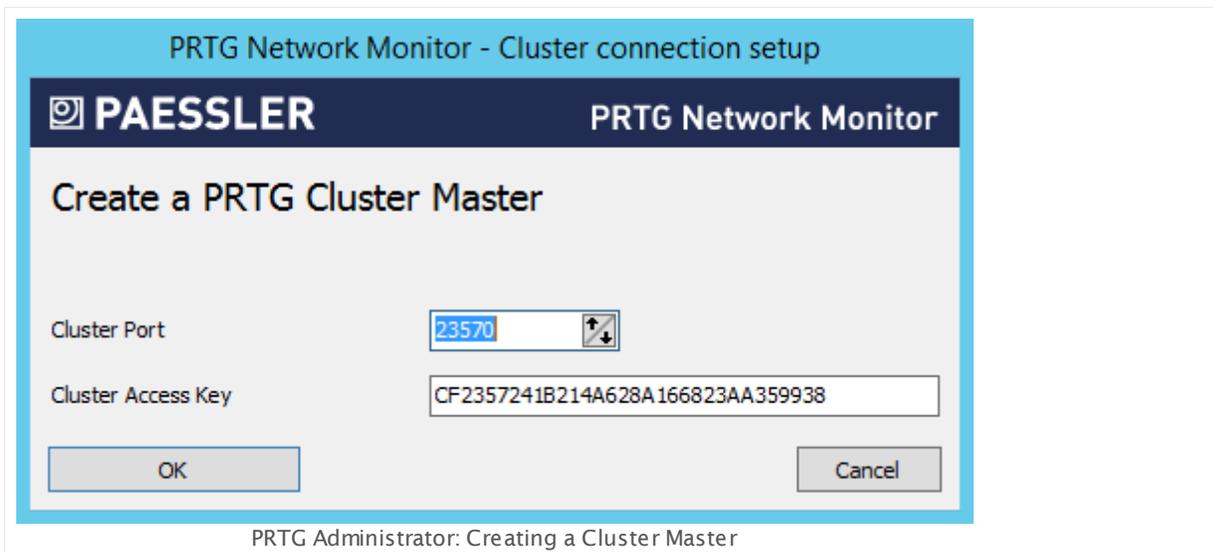
Create a PRTG Cluster...

- Click this button to start creating a cluster. The current PRTG core server will then be the **Master Node** of your cluster.
- Click **Yes** to confirm the conversion of this installation into a cluster master node.

Part 13: Advanced Topics | 10 Failover Cluster Configuration
1 Failover Cluster Step by Step



- A new dialog box will appear.



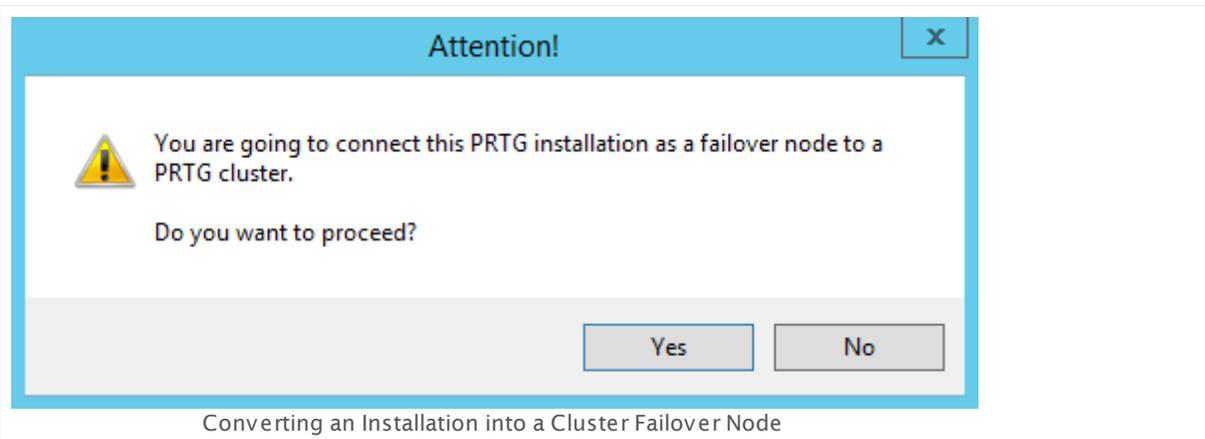
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.
- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- We recommend that you use the default value.
- Save the **Cluster Access Key** so you have it at hand when configuring your **Failover Node(s)**.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Step 3: Configure Failover Node

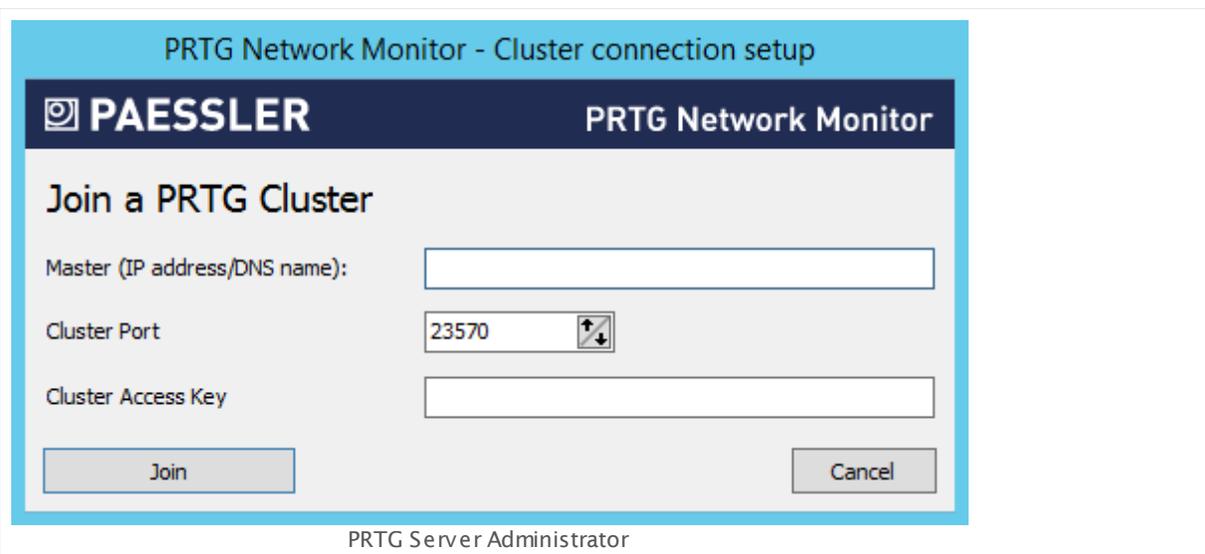
On the server that will be your Failover Node, open the [PRTG Administration Tool](#)³⁵⁶⁸. On the Cluster tab, click the following button:

Join a PRTG Cluster...

- Click this button to add this installation to an existing cluster that already has a **Master Node**. The current PRTG core server will then be a **Failover Node** in the cluster.
- This button is also available if you are currently running your PRTG installation in **Cluster Mode: Master Node**. This option will then change your master node to a failover node!
- Click **Yes** to confirm the conversion of this installation into a failover node.



- A dialog box will appear.



- Enter a **Master IP address/DNS name** for your cluster. It must be reachable from the machine running the failover node.
- Enter the other settings as defined in the settings of your **Master Node**. Please make sure you use the same settings on all nodes in your cluster.
- Enter a **Cluster Port**. This is the port on which the internal communication between the different cluster nodes is sent. Make sure connections between cluster nodes are possible on the selected port.

Part 13: Advanced Topics | 10 Failover Cluster Configuration

1 Failover Cluster Step by Step

- Enter or paste a **Cluster Access Key**. This is a unique access key. All nodes in a cluster have to be configured with the same cluster access key in order to join the cluster. Connection attempts with the wrong access key will be rejected.
- After confirming your settings you will be asked to restart Windows services. Please do so in order for your changes to take effect.

Step 4: Confirm Failover Node

Now you need to confirm the new failover node by setting it to **Active** in the master node's settings.

In a browser window, log in to the PRTG [web interface](#)^[168] of the **Master Node** server.

In the [System Administration—Cluster](#)^[3394] settings, you will see your “Master Node” server in the first line of the cluster list and your “Failover Node” server below.

i If you use [remote probes](#)^[3709] outside your local network, for each core server in the cluster use a DNS name or IP address that the probes can reach from the outside. Enter the entries in the [Cluster Node Setup](#)^[3394] table accordingly (see below). The addresses must be valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Remote probes outside your LAN cannot reach private IP addresses or DNS names!

Node Name	Node ID	Node State	IPs/DNS Names used for Connections Between Nodes
1 PRTG Network Monitor (10.0.1)	85F...	Active	#2 ⇒ #1 10.0.10.34
2 Node 10.0.10.35	CF0...	<input type="radio"/> Active <input checked="" type="radio"/> Inactive	#1 ⇒ #2 10.0.10.35
3		<input type="radio"/> Active <input checked="" type="radio"/> Inactive	#1 ⇒ #3 #2 ⇒ #3
4		<input type="radio"/> Active <input checked="" type="radio"/> Inactive	#1 ⇒ #4 #2 ⇒ #4
5		<input type="radio"/> Active <input checked="" type="radio"/> Inactive	#1 ⇒ #5 #2 ⇒ #5

IPs/DNS Names used for Connections

#2 ⇒ #1
10.0.10.34

#1 ⇒ #2
10.0.10.35

System Administration: Cluster Node Setup

For the “Failover Node”, set the radio button for **Node State** to **Active** and **Save** the changes. The nodes will now connect and exchange configuration data. This may take a few minutes.

Step 5: Check Cluster Connection

In two browser windows, log in to the PRTG web interfaces of **both** of your PRTG installations. Open the cluster status page in both windows by clicking on the narrow cluster information bars at the top of each window. You should see a cluster status with your two nodes in a **Connected** state after a few minutes.

Node 1: PRTG Network Monitor (10.0.10.34)		
Primary Node (Current Master)		Start Maintenance Mode
Connection To	IP	State
⇒ Node 10.0.10.35	10.0.10.35	Connected
Node 2: Node 10.0.10.35		
Secondary Node (Failover Node, Version: 50186)		Start Maintenance Mode
Connection To	IP	State
⇒ PRTG Network Monitor (10.0.10.34)	10.0.10.34	Connected

PRTG Cluster Status

Step 6: Trouble Shooting

Having any problems? If your nodes cannot connect, please see

- the cluster log entries on the [PRTG Status—Cluster Status](#) ³⁴¹² page of the web interface
- the core server logfile, a text file in the logs directory of your PRTG data folder (see section [Data Storage](#) ³⁷³⁴).

In the latest entries of these logs, you can see messages about any errors that might have occurred. These will give you hints on where to find a solution.

If you encounter connection problems between the two cluster nodes, please make sure no software or hardware firewall is blocking communication on the cluster port defined during cluster setup. Communication between the nodes must be possible in **both directions** in order for the cluster to work properly.

Step 7: Move Sensors to the Cluster Probe Now

That's it. You have successfully set up your failover cluster. All devices that you create or move under the **Cluster Probe** are monitored by both servers.

To monitor your existing configuration via all cluster nodes, on your master node, please move your groups, devices, and sensors from the local probe to the cluster probe! Objects, including their settings, will then be transferred to all cluster nodes automatically.

Step 8: Move Custom Content to Failover Nodes

On startup of the cluster master node, [maps](#) and [custom lookups](#) are automatically transmitted to the failover nodes. While changes to maps are automatically synchronized, you have to manually [\(re-\)load lookups](#) on all nodes. Other custom content has to be copied manually from the according [folders](#) on the master node to the same folders on the failover nodes:

- [Device templates](#): \devicetemplates subfolder of PRTG
- [Custom sensors](#): \Custom Sensors subfolder of PRTG
- [MIB files](#): \MIB subfolder of PRTG
- [SNMP libraries](#): \snmplibs subfolder of PRTG
- [Notifications](#): \Not ifications subfolder of PRTG
- The \webroot subfolder of PRTG if you customized the PRTG web interface, for example

Add More Failover Nodes

If you want to add an additional failover node to your cluster, you will need an additional license key for two and three failover nodes, and two additional license keys to run four failover nodes.

i In a cluster, only core servers running on the same size of [license](#) can be combined. For example, you can use several "PRTG 5000" licenses or several "PRTG 1000" licenses in one cluster. To add another failover node to your cluster, please set up a new PRTG core server installation on a new server, using an additional license key. Then proceed with [Step 3](#) and following. Use a second license key to set up both your second and third failover node, and use a third license key to set up your fourth failover node. Each failover cluster is technically limited to five cluster nodes: as a maximum, you can run one master node and four failover nodes in one cluster.

i Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not supported. For each additional failover node, divide the number of sensors by two.

More

Knowledge Base: My PRTG Cluster is messed up. How can I start over?

- <https://kb.paessler.com/en/topic/41903>

Advanced Topics

- [Active Directory Integration](#)
- [Application Programming Interface \(API\) Definition](#)

- [Filter Rules for xFlow, IPFIX, and Packet Sniffer Sensors](#)  3688
- [Channel Definitions for xFlow, IPFIX, and Packet Sniffer Sensors](#)  3690
- [Define IP Ranges](#)  3692
- [Define Lookups](#)  3693
- [Regular Expressions](#)  3704
- [Add Remote Probe](#)  3707
- [Failover Cluster Configuration](#)  3720
- [Data Storage](#)  3734
- [Using Your Own SSL Certificate](#)  3736
- [Calculating Percentiles](#)  3706

13.11 Data Storage

PRTG stores the monitoring configuration, monitoring data, logs, tickets, and reports, as well as support and debug data into different folders on the core server or the system running a [Remote Probe](#)³⁷⁰⁷. Additionally, there is data from PRTG in the program directory (for example, scripts for your [custom sensors](#)³¹⁵⁵) and in the Windows registry.

 You can find data in different locations. For detailed information, see this Knowledge Base article: [How and where does PRTG store its data?](#)

 You cannot access these directories on the PRTG hosted by Paessler core server system.

PRTG Program Directory

32-bit systems:

```
%programfiles%\PRTG Network Monitor
```

64-bit systems:

```
%programfiles(x86)%\PRTG Network Monitor
```

 These are the default paths. If you specified another installation directory, you will find your data there.

PRTG Data Folder

On Windows Vista (not officially supported), Windows 7, Windows 2008 R2, Windows 8, and Windows 2012:

```
%programdata%\Paessler\PRTG Network Monitor
```

On Windows XP and Windows Server 2003 (both are not officially supported):

```
%ALLUSERSPROFILE%\Application data\Paessler\PRTG Network Monitor
```

 These are the default paths, depending on your Windows version. If you specified a custom path for data storage, please look it up in the [PRTG Administration Tool](#)³⁵⁶⁶. Open this application and switch to the **Core Server** tab. You will find the path there.

Windows Registry

System settings on 32-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor
```

System settings on 64-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor
```

Enterprise Console settings:

```
HKEY_CURRENT_USER\Software\Paessler\PRTG Network Monitor\WinGUI
```

HTTP Full Web Page Sensor: Cached Files

If you use the HTTP Full Web Page Sensor, files might be cached in this directory;

```
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.
```

More

Knowledge Base: How and where does PRTG store its data?

- <https://kb.paessler.com/en/topic/463>

13.12 Using Your Own SSL Certificate with PRTG's Web Server

This section gives you a brief overview on how to use your own trusted SSL certificate files with the PRTG web server.

 This only applies to PRTG on premises instances, not to PRTG hosted by Paessler.

What is SSL?

PRTG supports Secure Sockets Layer (SSL) to encrypt all data entered and shown in the [Web Interface](#)^[166], in the [Enterprise Console](#)^[3430], or in the [Smartphone Apps](#)^[3484]. This ensures that no sensitive information can be intercepted when sending data between the PRTG core server and your client software.

By default, PRTG is already delivered with an SSL certificate so you can use secure connections to your PRTG core server. However, these certificate files are not signed by a valid authority, which is why browsers show an [SSL Certificate Warning](#)^[172] when you try to access the web interface. Despite this warning your connection is still encrypted successfully.

To remove the browser warning, you can obtain a certificate that is valid for your own domain name and signed by a valid authority. You can request your own trusted certificate from an issuer like GoDaddy, DigiCert, or InstantSSL, for example. The certificate must be provided in a suitable format and you have to import it correctly for your PRTG server.

Importing Trusted SSL Certificates for PRTG

There are many different issuers for certificates, and there are different formats certificates can be provided in. PRTG needs three different files, named correctly, containing data in the expected encoding and format. This can make the manual import of an issued certificate slightly complicated, because there are various certificate files that you must retrieve from a [certificate authority \(CA\)](#). So, to ease the installation of a trusted certificate, we provide the freeware tool **PRTG Certificate Importer**.

The PRTG Certificate Importer combines and converts all files that a CA bundle contains automatically for the use with PRTG and stores the certificate files into the correct path on your PRTG server. In the best case, you just provide the path to your received CA bundle and let the tool do the rest. We strongly recommend that you use the PRTG Certificate Importer if you want to install a trusted certificate for PRTG!

 For more information about this tool and a download link, see the Paessler website: [PRTG Certificate Importer](#)

Manual Certificate Import

Although we recommend that you use the PRTG Certificate Importer because it is much more comfortable, you still can import your trusted certificate manually. If you do so, please note that PRTG requires three different certificate files in a PEM encoded format and an unencrypted private key:

- **prtg.crt**: This is the certificate for your PRTG server. It has to be stored in **PEM** encoded format.

- **prtg.key**: This is the private key matching your server certificate. It has to be stored in **PEM** encoded format and may not be encrypted! Please make sure that you provide this file in **decrypted** format! The best way to check this is to open the file in a text editor. If you find a line containing the word "ENCRYPTED", the file still needs to be decrypted before you can use it with PRTG. Please decrypt using an SSL tool (for example, OpenSSL) and your key password.
- **root.pem**: This is the public root certificate of your certificate's issuer. It has to be stored in **PEM** encoded format and must contain all necessary root certificates of your issuer in one file. If there is more than one PEM encoded root certificate, please use a text editor to copy all of them into a single file (the order does not matter).

 PEM encoded files must not contain Unix line breaks! Only Windows line breaks are supported.

Once ready, copy these three files to the **/cert** sub folder of your PRTG program directory (please backup existing files) and restart your PRTG core server service (see [PRTG Administration Tool](#)³⁵⁸⁷).

 PRTG services will not be able to start if the files are not provided in exactly the expected format!

 For detailed instructions and examples, installation descriptions for various certificates (including **Wildcard** certificates), as well as links to certificate tools and converters, see the [More](#)³⁷³⁷ section below.

More

Freeware Network Tools: PRTG Certificate Importer—Installing Trusted SSL Certificates for PRTG Network Monitor

- <https://www.paessler.com/tools/certificateimporter>

Knowledge Base: How can I establish a secure web interface connection to PRTG?

- <https://kb.paessler.com/en/topic/273>

Knowledge Base: How can I use a trusted SSL certificate with the PRTG web interface?

- <https://kb.paessler.com/en/topic/283>

Part 14

Appendix

14 Appendix

Please find further information about PRTG and used terms in the following sections.

- [Glossary](#) 
- [List of Abbreviations](#) 
- [List of Icons](#) 
- [Support and Troubleshooting](#) 
- [Legal Notices](#) 
- [Differences between PRTG on premises and PRTG hosted by Paessler](#) 

14.1 Glossary

This section explains special words used in the context of PRTG Network Monitor.

i Here, only explanations are given. For information on where to find detailed instructions for a specific key word, see the **Index** section.

Alarms

The alarms list shows all [sensors](#) that are currently in a **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, or **Unusual** [status](#). This is useful for keeping track of all irregularities in your network.

Auto-Discovery

The auto-discovery process scans your network for [devices](#) using Ping (for [groups](#) only), it assesses the device type for all discovered devices, and it creates [sensor](#) sets that match the discovered device types based on built-in templates or your custom device templates.

Channel

The monitoring data of a [sensor](#) is shown in sensor channels. For example, for sensors that measure network traffic, there is one channel each for traffic **in**, traffic **out**, and traffic **total**. You can set various [triggers](#) for each channel, so you can define [sensor status](#) changes or [notifications](#) based on the monitoring data received.

Cluster

You can configure PRTG as a failover cluster for fail-safe monitoring. In a cluster, one or more [core servers](#) work together in one configuration. Every [node](#) can monitor every [device](#) in a network for gapless monitoring, so you can additionally compare monitoring results measured from different perspectives. This feature is not available in PRTG hosted by Paessler.

Cluster Node

Sometimes used as synonym for [Node](#).

Cluster Probe

When running PRTG in [cluster](#) mode, a cluster probe is automatically created. All [objects](#) created on the cluster probe or below in the [device tree](#) are monitored by all [nodes](#) in the cluster. Create or move [objects](#) there to monitor them fail-safely. If one node fails, the other nodes will continue to monitor them. You can add [groups](#) and [devices](#) to the cluster probe. On a PRTG installation, the cluster probe runs as part of this installation's [local probe](#). Your [remote probes](#) can send monitoring data to your cluster nodes so you can view the data of each probe on each cluster node.

Core Server

The central unit of PRTG. It receives monitoring data from the [probe\(s\)](#) and handles reporting and notifications, provides the web server for the user interfaces, and many other things. In a [cluster](#), one core server is installed on every node. The core server is configured as a Windows service that is permanently run by the Windows system without the requirement for a logged in user

Dashboard

In the **Home** menu of the web interface, there are several pre-configured dashboards available that show a quick overview of the overall status of your monitoring configuration. You can create custom dashboards using the [Maps](#) function.

Device

A device in PRTG represents a "real" physical device in the network. For an easily understandable tree structure, you usually create one PRTG device for each physical device you want to monitor (exceptions apply to some sensors that you can only create on the [local probe](#) device, and for sensor types that are not bound to a certain device, such as HTTP sensors, which are also usually created on the local probe). You can add one or more [sensors](#) on every device.

Device Template

If you want to add a certain [device](#) several times, you can create a device template from an existing device in your [device tree](#). When creating a device template, PRTG will save information for nearly all [sensors](#) on this device to a template file that you can later use in combination with [Auto-Discovery](#) (restrictions apply for a few sensor types).

Device Tree

The configuration of PRTG is represented in a hierarchical tree structure, the device tree, containing all [objects](#). While building the tree, you can relate to your network's topology to make your monitoring setup easy to understand.

Enterprise Console

The Enterprise Console (in old PRTG versions called "Windows GUI") is one alternative interface that you can use to connect to the PRTG [core server](#) to configure your setup, view monitoring results, and keep an eye on your network. It is a native Windows application for fast access to data and monitoring management.

Failover Master (Node)

If the [primary master](#) node fails, a [failover node](#) is promoted to current failover master and takes over the master role until the primary master node re-joins the [cluster](#).

Failover Node

In a [cluster](#), a failover node monitors all [sensors](#) on the [cluster probe](#), providing monitoring data for the [core server](#). Additionally, it serves as a backup in case the [master node](#) fails.

Geo Maps

Geo Maps show the different locations of your [devices](#) on a map, depending on the location data that you provide in the settings of [probes](#), [groups](#), or devices. The tiles on the maps that represent your devices also show the overall status of a location. This is useful for monitoring distributed networks.

Group

A group is an organizational unit in your PRTG tree structure that helps to arrange your [devices](#). You can add devices or additional sub-groups to existing [groups](#). This way you can model your physical network's topology within the PRTG configuration. You can use groups to arrange similar objects so that they inherit the same settings.

Hosted Probe

The hosted probe relates to PRTG hosted by Paessler like the [local probe](#) relates to PRTG on premises. When creating a PRTG hosted by Paessler instance, the system automatically adds the hosted probe. The hosted probe is always running on the PRTG [core server](#) system that we host for you and shows monitoring values of your PRTG instance hosted by Paessler. You can use the hosted probe to monitor [devices](#), servers, and services that are publicly accessible in the internet like, for example, websites. To monitor your Local Area Network (LAN), you need at least one [remote probe](#) installation in your network. The local probe is not available in PRTG hosted by Paessler.

Library

Libraries are a way to show parts of your [device tree](#) in a different layout or with different filters enabled. There is an editor available that allows you to create libraries directly in your browser.

Library Node

[Libraries](#) use library nodes to reference [objects](#) in your monitoring setup. Library nodes can show a subtree of the [device tree](#) in the library or they can show a collection of filtered [sensors](#) in the library.

Local Probe

When installing PRTG on premises, the PRTG local probe is installed together with the PRTG [core server](#). All [objects](#) created on the local probe, or below it in the [device tree](#), are monitored by the local core system. You can add [groups](#) and [devices](#) to the probe. If you use PRTG hosted by Paessler, the [hosted probe](#) replaces the local probe. There are some [differences between PRTG hosted by Paessler and PRTG on premises](#).

Lookup

PRTG uses lookups for some [sensor](#) types and for some sensors with custom [channels](#). In general, lookups make data more human friendly because they map status values as returned by a [device](#) (usually integers) to more informative expressions in words that show you the status of a monitored device as a clear message.

Map

Maps (sometimes referred to as "[dashboard](#)") are a way to present monitoring data the way you want to arrange it. There is an editor available that allows creating maps directly in your browser. Using this unique concept, you can also make your overview pages of live data publicly available.

Master Node

In a [cluster](#), the master node controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node, which distributes the changes to all other nodes in real time.

Meta-Scan

Sensors that use the meta-scan function, for example SNMP sensors, first look at the [device](#) to find what can be monitored. This can be tables, OIDs, or disks, for example. When the meta-scan is done, the second step of the [Add Sensor](#) dialog shows you the parameters that you can monitor. Some sensors require basic information before they can perform a meta-scan. Provide the requested information, such as credentials, in the appearing window. PRTG will then scan and recognize all parameters available for monitoring based on your input.

Mini Probe

PRTG Mini Probes allow you to create small [probes](#) on any [device](#) (not just on Windows systems).

Node

In a [cluster](#), there is one [master node](#) and one or more [failover nodes](#). On each node, one PRTG [core server](#) installation is running independently. All nodes are connected to each other, exchanging configuration and monitoring data.

Notification

PRTG uses notifications to send you alerts whenever PRTG discovers a defined status, such as slow or failing [sensors](#)^[3747], or when sensor [channels](#)^[3741] breach threshold values. You can define an unlimited number of notifications allowing the use of one, or more, of several communication channels like email, text messaging, push notifications to Android and iOS devices, and many more.

Object

All different items in the [device tree](#)^[3742] are generally referred to as objects or monitoring objects. An object can be a [probe](#)^[3745], a [group](#)^[3743], a [device](#)^[3742], or a [sensor](#)^[3747].

Object Hierarchy

All [objects](#)^[3745] are arranged in a hierarchical order that makes it easier to navigate and arrange settings. The object hierarchy is used to define common settings for groups of objects.

Object Selector

The object selector enables you to browse all [objects](#)^[3745] in your configuration and select an object in two steps. The left-hand side shows your [device tree](#)^[3742]. If you have selected a [device](#)^[3742], the right hand side shows the [sensors](#)^[3747] on the device.

Primary Master (Node)

The **primary** master node in a [cluster](#)^[3741] is the [node](#)^[3744] that is master by configuration. Only if it fails, one of the [failover nodes](#)^[3743] becomes [failover master](#)^[3742] and takes over the master role until the primary master node re-joins the cluster.

Probe

On a probe, the actual monitoring takes place. A probe can run as [local probe](#)^[3744] on the local system where the [core server](#)^[3742] is installed. There are also [cluster probes](#)^[3741], [remote probes](#)^[3746], and [hosted probes](#)^[3743].

Probe Device

This is an internal system device that PRTG automatically adds to the [local probe](#)^[3744]. It has access to the computer where the probe is running and monitors its health parameters using several [sensors](#)^[3747].

PRTG Administration Tool

The PRTG Administration Tool is part of your PRTG installation and helps you edit administrative settings of your [local probe](#)^[3744] and your [remote probe](#)^[3746] installations. You can launch the PRTG Administration Tool from the Windows start menu, on your [core server](#)^[3742], or on your remote probe server.

PRTG Application Programming Interface (API)

The PRTG Application Programming Interface (API) enables you to access monitoring data and manipulate [objects](#) using HTTP requests, run your own written [sensors](#) and [notifications](#), and implement [Mini Probes](#).

PRTG hosted by Paessler

PRTG hosted by Paessler is the PRTG cloud solution where we at Paessler run the [core server](#) and [hosted probe](#) for you. No core server installation inside your network is necessary. The PRTG web interface for monitoring configuration and reviewing monitoring data is the same for both PRTG hosted by Paessler and PRTG on premises.

PRTG on Premises

PRTG on premises is a powerful network monitoring application for Windows-based systems that allows you to monitor your entire network. A [core server](#) installation inside your network is necessary. The PRTG web interface for monitoring configuration and reviewing monitoring data is the same for both PRTG on premises and PRTG hosted by Paessler.

Recommended Sensors Detection

With the [sensor](#) recommendation engine, PRTG can analyze [devices](#) in your network and suggest sensors that are still missing for a complete monitoring. The analysis runs with low priority in the background when you add a new device, when the last analysis was executed more than 30 days ago, or when you manually start it.

Release Channel

PRTG updates are delivered in different release channels. With PRTG on premises, you can choose between maximum stability (Stable), or most early access to new features (Canary or Preview). PRTG hosted by Paessler does not have release channels. Instead, we roll out the latest stable version to PRTG hosted by Paessler instances in stages, so your instance automatically updates to the latest stable version.

Remote Probe

A remote probe is a small piece of software installed on a computer in the local or remote network. It scans the network from there and sends monitoring results to the [core server](#). Once the connection is established, the remote probe is shown in the PRTG tree structure. All [objects](#) created on the remote probe, or below it in the [device tree](#), are monitored by the remote system running the remote probe. You can add [groups](#) and [devices](#) to the probe. In a [cluster](#), remote probes can connect to all cluster nodes so you can view monitoring data of a probe on all nodes.

Root Group

The root group is the topmost instance in the [object hierarchy](#) of PRTG. It contains all other [objects](#) in your setup. All other objects inherit the settings of the root group, making configuration easier later on.

Schedule

You can use schedules to pause monitoring/notification for certain time periods or at certain times. You can also use schedules to define the time periods that are to be covered when creating reports.

Sensor

A sensor monitors one aspect of a [device](#). For example, monitoring if a device responds to a Ping request is done by one sensor. Monitoring the traffic of one Ethernet port of a router device is done by another sensor. For monitoring the CPU load of the local system yet another sensor is set up, and so on. The data of sensors is shown in their respective [channels](#). Each sensor has at least one channel.

Sensor States

The color of a [sensor](#) always shows its current status. There are 8 different sensor states: **Down**, **Down (Partial)**, **Down (Acknowledged)**, **Warning**, **Unusual**, **Up**, **Paused**, and **Unknown**.

Sensor Tree

Sometimes used as synonym for [device tree](#).

Similar Sensors Detection

Similar sensors detection enables PRTG to analyze [sensor](#) data for similarities. The detection will run in the background with low priority. The recommended setting for similar sensors detection is to let PRTG automatically decide how many [channels](#) will be analyzed.

Tickets

[Tickets](#) are created by the system or a PRTG user and contain important messages or action steps for the administrator or another specific user to take. Every ticket should be viewed to take appropriate action. You can access the list of tickets from the main menu.

Toplist

Packet Sniffer and xFlow [sensor](#) types can break down the traffic by IP address, port, protocol, and other parameters. The results are shown in graphs that are known as Toplists.

Trigger

PRTG sends a [notification](#) when a defined event evokes it. These events are known as triggers. The following events can trigger notifications: [sensor status](#) changes, [sensor](#) value threshold breaches, speed threshold breaches, volume threshold breaches, and sensor value changes.

Unusual Detection

The unusual detection can set [sensors](#) to an **Unusual status** when there are values that are untypical for the time span in which they are measured. PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor will indicate this with the **Unusual** status.

xFlow

Paessler designates all kinds of flow protocols as xFlow. Currently, PRTG supports NetFlow V5 and V9, IPFIX, sFlow V5, and jFlow V5.

14.2 List of Abbreviations

Please see below for a list of abbreviations used in this documentation.

ADO: ActiveX Data Objects (ADO)

ADSL: Asymmetric Digital Subscriber Line (ADSL)

AJAX: Asynchronous Java Script and XML (AJAX)

API: Application Programming Interface (API)

CBQoS: Class Based Quality of Service (CBQoS)

cDOT: clustered Data ONTAP (cDOT)

CGI: Common Gateway Interface (CGI)

CIFS; Common Internet File System (CIFS)

CLI: command-line interface (CLI)

CoS: Class of Service (CoS)

CSV: Comma Separated Values (CSV)

DAG: Database Availability Group (DAG)

DHCP: Dynamic Host Configuration Protocol (DHCP)

DMZ: Demilitarized Zone (DMZ)

DSCP: Differentiated Services Code Point (DSCP)

DNS: Domain Name Service (DNS)

DSCP: Differentiated Services Code Point (DSCP)

FAT: File Allocation Table (FAT)

FTP: File Transfer Protocol (FTP)

FTPS: FTP over SSL (FTPS)

FQDN: Fully Qualified Domain Name (FQDN)

GID: global ID (GID)

GUI: Graphical User Interface (GUI)

GUID: Globally Unique Identifier (GUID)

HTTP: Hypertext Transfer Protocol (HTTP)

HTTPS: Hypertext Transfer Protocol Secure (HTTPS)

ICMP: Internet Control Message Protocol (ICMP)

ICPIF: Impairment Calculated Planning Impairment Factor (ICPIF)

iDRAC: Integrated Dell Remote Access Controller (iDRAC)

IIS: Microsoft Internet Information Services (IIS)

iLO: HP Integrated Lights-Out (iLO)

IMAP: Internet Message Access Protocol (IMAP)

IPFIX: IPFIX (Internet Protocol Flow Information Export)

IPMI: Intelligent Platform Management Interface (IPMI)

IPsec: Internet Protocol Security (IPsec)

iRMC: integrated Remote Management Controller (iRMC)

iSCSI: internet Small Computer System Interface (iSCSI)

JSON: JavaScript Object Notation (JSON)

LAN: Local Area Network (LAN)

LDAP: Lightweight Directory Access Protocol (LDAP)

MIB: Management Information Base (MIB)

MoID: Managed Object ID (MoID)

MOS: Mean Opinion Score (MOS)

MSP: Managed Service Provider (MSP)

NAS: Network Attached Storage (NAS)

NAT: Network Address Translation (NAT)

NFS: Network File System (NFS)

NSA: Network Security Appliance (NSA)

NTFS: New Technology File System (NTFS)

NTLM: NT LAN Manager (NTLM)

OID: Object Identifier (OID)

OMSA: OpenManage Server Administrator (OMSA)

PDF: Portable Document Format (PDF)

PDV: Packet Delay Variation (PDV)

POP3: Post Office Protocol version 3 (POP3)

QoS: Quality of Service (QoS)

RADIUS: Remote Authentication Dial-In User Service (RADIUS)

REST: Representational State Transfer (REST)

RMON: Remote Monitoring (RMON)

RPC: Remote Procedure Call (RPC)

RTT: Round Trip Time (RTT)

SaaS: Software as a Service (SaaS)

SAN: Storage Area Network (SAN)

SASL: Simple Authentication and Security Layer (SASL)

SCVMM: System Center Virtual Machine Manager (SCVMM)

SIP: Session Initiation Protocol (SIP)

SLA: Service Level Agreement (SLA)

S.M.A.R.T.: Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.)

SMB: Server Message Block (SMB)

SMTP: Simple Mail Transfer Protocol (SMTP)

SNI: Server Name Identification (SNI)

SNMP: Simple Network Management Protocol (SNMP)

SNTP: Simple Network Time Protocol (SNTP)

SOAP: Simple Object Access Protocol (SOAP)

SPAN: Switched Port Analyzer (SPAN)

SQL: Structured Query Language (SQL)

SRP: Secure Remote Password (SRP)

SSH: Secure Shell (SSH)

SSL: Secure Sockets Layer (SSL)

SSO: Single Sign-On (SSO)

TCP: Transport Control Protocol (TCP)

TFTP: Trivial File Transfer Protocol (TFTP)

TLS: Transport Layer Security (TLS)

UAC: User Account Control (UAC)

UCS: Unified Computing System (UCS)

UDP: User Datagram Protocol (UDP)

UNC: Uniform Naming Convention (UNC)

UPnP: Universal Plug and Play (UPnP)

UTC: UTC (Coordinated Universal Time)

UUID: Universally Unique Identifier (UUID)

VoIP: Voice over IP (VoIP)

VPN: Virtual Private Network (VPN)

WAN: Wide Area Network (WAN)

WBEM: Web-Based Enterprise Management (WBEM)

WMI: Windows Management Instrumentation (WMI)

WQL: Windows Management Instrumentation Query Language (WQL)

WSUS: Windows Server Update Services (WSUS)

XML: Extensible Markup Language (XML)

14.3 List of Icons

Please see below for a list of icons used in this documentation.



There is more detailed information on how this feature works exactly.



This feature is in beta status and may not function properly in all situations.



There is more information on this topic in another section in the PRTG manual.



There is more information on this topic in the Paessler Knowledge Base.



Notes that contain information about potential errors and that offer tips on how to keep them from occurring.



Notes that contain extremely critical information. Pay close attention to these notes, otherwise they could have serious consequences.



Notes that contain critical information. Pay close attention to these notes, otherwise PRTG might not function properly.



Notes that contain additional information.



Step-by-step instructions.



Examples on how to use a feature.



Calls to action. These contain tips, requirements, or instructions on what you need to enter in certain fields, or inform you that certain programs or apps need to be installed.



This information is relevant for PRTG hosted by Paessler.



This information is relevant for PRTG on premises.

14.4 Support and Troubleshooting

Need help with PRTG? There are several ways to get support and troubleshoot.

Video Tutorials

A video says more than a thousand words—watch tutorials for PRTG from Paessler and other PRTG users.

- <https://www.paessler.com/support/videos>

Paessler Knowledge Base

In the Knowledge Base, you can search in hundreds of articles about PRTG. You can post your own questions and answers, too!

- <https://kb.paessler.com>

Open a Support Ticket

Users that have purchased a license can open support tickets, which will usually be answered by Paessler's staff in less than 24 hours on business days. Please use the [support form](#)³⁴²⁴ that is available in PRTG to contact our support team. This is the best way to get detailed help quickly. If you cannot use this form, contact us via our webpage.

- <https://shop.paessler.com/en/openticket>

14.5 Differences between PRTG on Premises and PRTG Hosted by Paessler

Please see below for the differences between the settings and features that PRTG on premises and PRTG hosted by Paessler have to offer.

Licensing, Payment, Infrastructure

TOPIC	PRTG ON PREMISES	PRTG HOSTED BY PAESSLER
Trial Period	30 days	10 days
Freeware	freeware (100 sensors) available	no freeware, smallest edition is PRTG 500
Payment	one-time license fee plus yearly maintenance	monthly fee
PRTG Edition Size Flexibility	upgrade only	upgrade or downgrade
Max. Installation Size	unrestricted	5,000 sensors
PRTG Update Management	done by user	done by Paessler
Enterprise Console	full support	not supported: connections are not possible

Features

FEATURE	PRTG ON PREMISES	PRTG HOSTED BY PAESSLER
Local Probe	☺	☹
Hosted Probe	☹	☺
Cluster	☺	☹

FEATURE	PRTG ON PREMISES	PRTG HOSTED BY PAESSLER
Customizations (CSS, HTML, lookups, maps, device icons)	😊	🚫
Freeware (100 sensors)	😊	🚫
RDP Access to Core Server	😊	🚫
Historic Data Purging (manually defined)	😊	🚫
Active Directory Integration	😊	🚫
License settings via PRTG web interface	😊	🚫
Recommended Sensors on Local Probe/Hosted Probe	😊	🚫
Auto-Discovery for groups on Local Probe/Hosted Probe	😊	🚫
Mini Probes	😊	🚫
Device Tools on Local Probe/ Hosted Probe	😊	🚫
Proxy Server settings	😊	🚫
System Information on Local Probe/Hosted Probe	😊	🚫
PRTG Administration Tool on PRTG Core Server	😊	🚫
MIB import and usage as oidlib with SNMP Library sensor	😊	🚫
MIB import for SNMP Trap Receiver sensor	😊	🚫
Notification types: <ul style="list-style-type: none"> ▪ SMS/Pager Message 	😊	🚫

FEATURE	PRTG ON PREMISES	PRTG HOSTED BY PAESSLER
<ul style="list-style-type: none"> ▪ Add Entry to Event Log ▪ Syslog Message ▪ SNMP Trap Message ▪ Execute Program 		
Re-login request on setup pages after 15 minutes	😊	🚫

Sensors on the Hosted Probe of PRTG hosted by Paessler

If you use PRTG hosted by Paessler, you can add the following sensors only to remote probes.

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
Active Directory Replication Errors Sensor	🚫
ADO SQL v2 Sensor	🚫
Dell PowerVault MDi Physical Disk Sensor	🚫
Dell PowerVault MDi Logical Disk Sensor	🚫
Enterprise Virtual Array Sensor	🚫
Event Log (Windows API) Sensor	🚫
Exchange Backup (PowerShell) Sensor	🚫
Exchange Database DAG (PowerShell) Sensor	🚫
Exchange Database (PowerShell) Sensor	🚫

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
Exchange Mailbox (PowerShell) Sensor	⊘
Exchange Mail Queue (PowerShell) Sensor	⊘
Exchange Public Folder (PowerShell) Sensor	⊘
EXE/Script Advanced Sensor	⊘
EXE/Script Sensor	⊘
File Content Sensor	⊘
File Sensor	⊘
Folder Sensor	⊘
HTTP Full Web Page Sensor	⊘
HTTP Push Count Sensor	⊘
HTTP Push Data Advanced Sensor	⊘
HTTP Push Data Sensor	⊘
Hyper-V Cluster Shared Volume Disk Free Sensor	⊘
Hyper-V Host Server Sensor	⊘
Hyper-V Virtual Machine Sensor	⊘
Hyper-V Network Adapter Sensor	⊘
Hyper-V Virtual Storage Sensor	⊘
IPFIX (Custom) Sensor	⊘
IPFIX Sensor	⊘

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
IPMI System Health Sensor	⊘
jFlow V5 (Custom) Sensor	⊘
jFlow V5 Sensor	⊘
Microsoft SQL v2 Sensor	⊘
MySQL v2 Sensor	⊘
NetFlow V5 (Custom) Sensor	⊘
NetFlow V5 Sensor	⊘
NetFlow V9 (Custom) Sensor	⊘
NetFlow V9 Sensor	⊘
Oracle SQL v2 Sensor	⊘
Oracle Tablespace Sensor	⊘
Packet Sniffer (Custom) Sensor	⊘
Packet Sniffer Sensor	⊘
PerfCounter Custom Sensor	⊘
PerfCounter IIS Application Pool Sensor	⊘
Port Range Sensor	⊘
Port Sensor	⊘
PostgreSQL Sensor	⊘
Python Script Advanced Sensor	⊘

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
QoS (Quality of Service) Round Trip Sensor	<input type="checkbox"/>
QoS (Quality of Service) One Way Sensor	<input type="checkbox"/>
sFlow (Custom) Sensor	<input type="checkbox"/>
sFlow Sensor	<input type="checkbox"/>
Share Disk Free Sensor	<input type="checkbox"/>
SMTP Sensor	<input type="checkbox"/>
SNMP Trap Receiver Sensor	<input type="checkbox"/>
Syslog Receiver Sensor	<input type="checkbox"/>
Windows MSMQ Queue Length Sensor	<input type="checkbox"/>
Windows Physical Disk I/O Sensor	<input type="checkbox"/>
Windows Print Queue Sensor	<input type="checkbox"/>
Windows Updates Status (PowerShell) Sensor	<input type="checkbox"/>
Windows CPU Load Sensor	<input type="checkbox"/>
WMI Custom Sensor	<input type="checkbox"/>
WMI Custom String Sensor	<input type="checkbox"/>
WMI Event Log Sensor	<input type="checkbox"/>
WMI Exchange Server Sensor	<input type="checkbox"/>
WMI Exchange Transport Queue Sensor	<input type="checkbox"/>

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
WMI File Sensor	⊘
WMI Free Disk Space (Multi Disk) Sensor	⊘
WMI HDD Health Sensor	⊘
Windows IIS 6.0 SMTP Received Sensor	⊘
Windows IIS 6.0 SMTP Sent Sensor	⊘
Windows IIS Application Sensor	⊘
WMI Logical Disk I/O Sensor	⊘
WMI Memory Sensor	⊘
Windows Network Card Sensor	⊘
Windows Pagefile Sensor	⊘
Windows Process Sensor	⊘
WMI Remote Ping Sensor	⊘
WMI Security Center Sensor	⊘
WMI Service Sensor	⊘
WMI SharePoint Process Sensor	⊘
WMI Share Sensor	⊘
Windows System Uptime Sensor	⊘
WMI UTC Time Sensor	⊘
WMI Vital System Data Sensor	⊘

SENSOR ON HOSTED PROBE	PRTG HOSTED BY PAESSLER
WMI Volume Sensor	
WSUS Statistics Sensor	
WMI Microsoft SQL Server 2005 Sensor (Deprecated)	
WMI Microsoft SQL Server 2008 Sensor	
WMI Microsoft SQL Server 2012 Sensor	
WMI Microsoft SQL Server 2014 Sensor	
WMI Microsoft SQL Server 2016 Sensor	
WMI Terminal Services (Windows 2008+) Sensor	
WMI Terminal Services (Windows XP/Vista/2003) Sensor	

Settings

SETTING TITLE	SETTING NAME	PRTG ON PREMISES	PRTG HOSTED BY PAESSLER
Auto-Update	When a New Version is Available		
	Installation Time		
	Release Channel		
Notifications	SMS/Page Message		

Part 14: Appendix | 5 Differences between PRTG on Premises and PRTG Hosted by Paessler

	Add Entry To Event Log	😊	🚫
	Syslog Message	😊	🚫
	SNMP Trap Message	😊	🚫
	Execute Program	😊	🚫
Core & Probes	Proxy Configuration	😊	🚫
	Probe Connection IPs	😊	🚫
	Mini Probes	😊	🚫
	Mini Probe Port	😊	🚫
Probe Administrative Tools	Restart Local Probe	😊	🚫
Scanning Intervals	Available Intervals (definition of individual intervals)	😊	🚫
Notification Delivery	SMTP Delivery (everything but sender email and name)	😊	🚫
	SMS Delivery	😊	🚫
Recommended Sensors Detection	Detection Engine	😊	🚫
User Interface (Website)	DNS Name	😊	🚫
	Google Analytics Tracking ID	😊	🚫
User Interface (Web Server)	IP Address for Web Server	😊	🚫
	TCP Port for Web Server	😊	🚫
	Web Server Port	😊	🚫
	Web Server Security	😊	🚫

Part 14: Appendix | 5 Differences between PRTG on Premises and PRTG Hosted by Paessler

	SSL Security	😊	🚫
	Currently Active IP Address/ Port Combination(s)	😊	🚫
User Accounts	Login Name	😊	🚫
	Password	😊	🚫
	Passhash	😊	🚫
Core Administrative Tools	Create Configuration Snapshot	😊	🚫
	Write Core Status File	😊	🚫
	Clear Caches	😊	🚫
	Load Lookups	😊	🚫
	Restart Core Server	😊	🚫
Advanced Network Analysis	System Information	😊	🚫
Scheduled Restart Settings (Local Probe)	Restart Options	😊	🚫
	Restart Schedule	😊	🚫
	Specify Day	😊	🚫
	Specify Hour	😊	🚫

14.6 Legal Notices

Build using Indy Internet Direct (<http://www.indyproject.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Uses the net-SNMP library, see "netsnmp-license.txt". Uses the DelphiZip library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (<http://www.delphizip.net/>). Uses FastMM (<http://sourceforge.net/projects/fastmm/>), TPLockBox (<http://sourceforge.net/projects/tplockbox>) and Delphi Chromium Embedded (<http://code.google.com/p/delphichromiumembedded/>) under the Mozilla Public License 1.1 (MPL 1.1, available from <http://www.mozilla.org/MPL/MPL-1.1.html>). Soundfiles from <http://www.soundsnap.com>. Uses Public Domain regional maps from the "CIA World Factbook" webpage of the CIA (<https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html>). Uses the "wkhtmltopdf" (<http://code.google.com/p/wkhtmltopdf/>) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see [wkhtmltopdf_lgpl-3.0.txt](#)). Icons from <http://www.androidicons.com>. Uses the IPMIUTIL library under the BSD 2.0 license, see "ipmi_bsd-2.0.txt". Uses PhantomJS, see "phantomjs-license.bsd".. Uses the Npgsql - .Net Data Provider for Postgresql library (for license information see [ipmi_bsd-2.0.txt](#)).

All product names, company names, and logos referenced to or depicted herein are the trademarks™, registered® trademarks, or service marks of the respective owners. Use of them, their occurrence, or references to their occurrence in graphical representations of the web interface herein is solely for informational purposes and does not imply any affiliation with or endorsement by the respective owners.

Privacy Policy

<https://www.paessler.com/company/privacypolicy>

General Business Terms and License Conditions

<https://www.paessler.com/company/terms>

Last manual export: Tuesday, August 14, 2018 7:46:45 PM

Last change to this manual (YYYY-MM-DD): 8/14/2018