4.4 Install a Cluster

PRTG offers one single failover cluster in all licenses, including the Freeware Edition. A single failover cluster consists of two machines (master node and failover node) that each run one installation of PRTG. They are connected to each other and exchange configuration and monitoring data. You can run a cluster with up to five cluster nodes.

This feature is not available in PRTG Hosted Monitor.

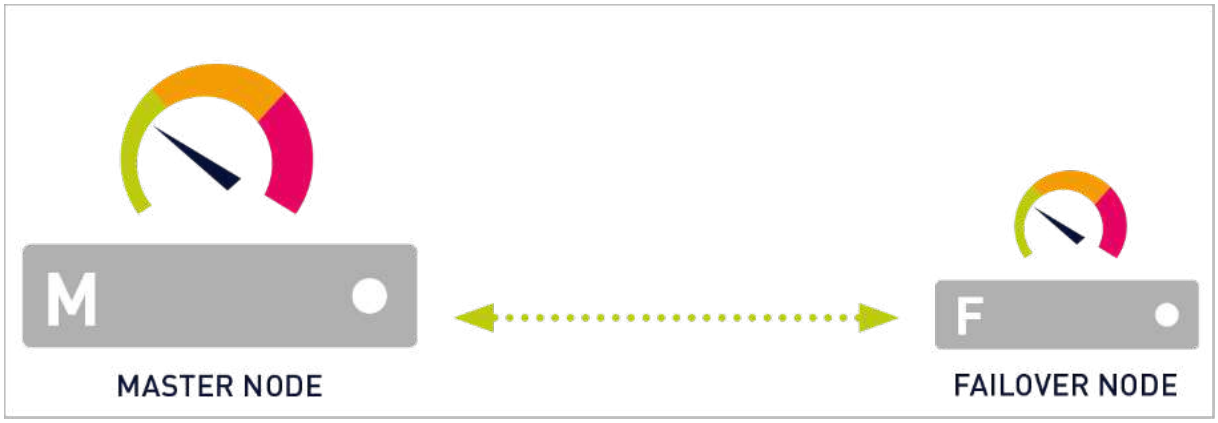


Illustration of a Single Failover Cluster

For more information, see section Failover Cluster Configuration 3631.

More

KNOWLEDGE BASE

What is the clustering feature in PRTG?

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

4.5 Enter a License Key

A license key for PRTG Network Monitor consists of the License Name and a License Key. The license key is a string that consists of 10 blocks with six characters each.

Your License Information

You have received the License Name (PRTG Network Monitor only) and the License Key from Paessler via email or in a license document in the Paessler Software Shop and Customer Service Portal. Copy this information and paste it when PRTG asks you to enter your license information in the setup dialog.

ⓘ You can find the label License Owner in some documents from the Paessler shop. License Owner is the same as License Name, for which you might be asked when you install PRTG or when you change your license key 102.

ⓘ For the Trial Edition and Freeware Edition, you receive the required license information on the Paessler web page when you download the Trial Edition of PRTG. For the Commercial Edition, use your commercial license information.

License Information	Example
License Name	Example Organization ⓘ Paessler PRTG Enterprise Monitor subscription licenses do not have a License Name.
License Key	P10000-FFSEJ3-ZHGRD5-UR1CS9-U73FG2-G645F1-YVF1D0-H83234

There are two license key types:

- Trial Edition/Freeware Edition license key: With a Trial Edition license key, you can experience unlimited functionality of PRTG during the 30-day trial period. Your installation automatically switches to the Freeware Edition afterward.
  For more information about how to get your free Trial Edition, see section Download PRTG 91.
- Commercial Edition license key: You can only enter this key if you have purchased the Commercial Edition. Your installation allows the number of sensors according to your license 21.

During the setup process for installing the Commercial Edition, PRTG asks you to enter your license information. We recommend that you copy and paste your license data. If you install the Trial Edition, you do not need to enter a license key.

Change License Key

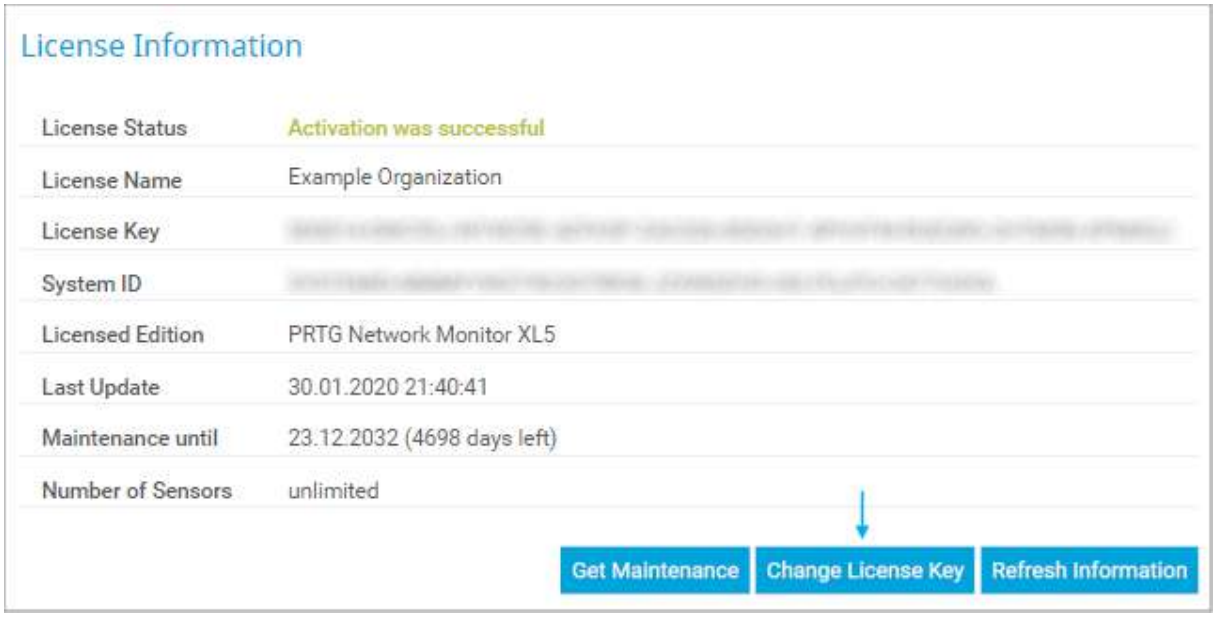
Because PRTG already asks for a key during installation, you usually do not need to manually enter one afterward. However, there are still scenarios where you need to change your key and activate the respective license. For example, you must provide your Commercial Edition license key if you have purchased the Commercial Edition and want to upgrade your Freeware Edition or Trial Edition, or if you upgrade a Commercial Edition license to a newer edition.

1. To enter a new license key, log in to the PRTG web interface 124.
2. Select Setup | License Information from the main menu bar 260.
3. Click Change License Key. The Update Your License page appears where you can activate your new license.
4. Select the activation type Automatic (online activation with optional HTTP proxy) if your PRTG core server can connect to the internet.
   ⓘ Without internet access, you must select Manual (offline activation). The activation process works a bit differently in this case and requires manual interaction. See section License Information 3399 for more information.
5. Enter your license information and click Update License.
6. PRTG connects to the Paessler activation server on port 443 and validates your license.

If everything works fine, you see the message Activation was successful as License Status at the top of the page.

For more information, see section License Information 3398.

ⓘ The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, see step 3 3399 on the Update Your License page. If the activation fails, you can also try an offline activation.



Update Your License: Click Change License Key

More

KNOWLEDGE BASE

How do I upgrade to a later edition of PRTG?

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

The automatic license activation of my PRTG Enterprise Monitor license does not work. What can I do?

- https://kb.paessler.com/en/topic/89281

4.6 Activate the Product

PRTG Network Monitor automatically activates your license via the internet during the installation process. If PRTG cannot access the activation server, you must manually activate your license.

ⓘ You must complete the product activation process once to use PRTG, otherwise it does not run. Do not forget to activate your commercial license when you want to upgrade your Trial Edition or Freeware Edition installation.

Online Activation

Because PRTG already asks for a key during installation, you usually do not need to manually enter one afterward. However, there are still scenarios where you need to change your key and activate the respective license. For example, you must provide your Commercial Edition license key if you have purchased the Commercial Edition and want to upgrade your Freeware Edition or Trial Edition, or if you upgrade a Commercial Edition license to a newer edition.

1. To enter a new license key, log in to the PRTG web interface 124.
2. Select Setup | License Information from the main menu bar 260.
3. Click Change License Key. The Update Your License page appears where you can activate your new license.
4. Select the activation type Automatic (online activation with optional HTTP proxy) if your PRTG core server can connect to the internet.
   ⓘ Without internet access, you must select Manual (offline activation). The activation process works a bit differently in this case and requires manual interaction. See section License Information 3399 for more information.
5. Enter your license information and click Update License.
6. PRTG connects to the Paessler activation server on port 443 and validates your license.

If everything works fine, you see the message Activation was successful as License Status at the top of the page.

For more information, see section License Information 3398.

ⓘ The PRTG core server needs an internet connection on port 443 to activate. If a proxy connection is needed, see step 3 3399 on the Update Your License page. If the activation fails, you can also try an offline activation.

Offline Activation

If no internet connection is available, you must activate PRTG manually:

1. In the PRTG web interface, select Setup | License Information from the main menu bar.
2. Click Change License Key. The Update Your License page appears where you can activate your license.
3. Select the activation type Manual (offline activation).
4. Enter your license information and follow the instructions of step 3b 3400 and step 4 3400 on the Update Your License page.

5. Click Update License.

If the activation was successful, you see the message Activation was successful as License Status at the top of the page.

For more information, see section License Information 3398.

If your PRTG core server is offline, you need to manually activate your license after you renew your maintenance. This ensures that you can install updates, for example. Your maintenance information has to be the same as in the PRTG installer, so you need to activate your license offline before you install an update.

More

KNOWLEDGE BASE

Which servers does PRTG connect to for software auto-update, activation, etc.?

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

4.7 Install a Remote Probe

Remote probes can extend your monitoring with PRTG.

- With remote probes, you can monitor different subnetworks that are separated from your PRTG core server by a firewall, and you can keep an eye on remote locations. You can install one or more remote probes 3621.
- Remote probes are useful if you want to distribute monitoring load by taking it from the PRTG core server system and putting it on one or more remote probe systems.
- You need a remote probe if you want to monitor your local network with a PRTG Hosted Monitor instance.

ⓘ PRTG automatically updates remote probes but, in rare cases, you must manually update remote probes. You receive a ToDo ticket 211 in this case. Follow the steps below 106 to manually update remote probes.

ⓘ If you run PRTG in a cluster, see Cluster and Remote Probes Outside the LAN 109 in this section.

If you have issues after the installation, see section Debugging Remote Probe Connection Issues 115 .

For a partially automatic installation of a remote probe directly from the device tree in the PRTG web interface, see section Remote Probe Setup via Device Tools 3625. For a quick installation guide, see the Paessler website: How to install a PRTG remote probe in 4 steps.

Steps to Take

To install a remote probe with the Remote Probe Installer, follow these steps:

- Step 1: Meet the Requirements 106
- Step 2: Prepare the PRTG Core Server 107: start here if you use PRTG Network Monitor
- Step 3: Download the Remote Probe Installer from the PRTG Web Interface 109: start here if you use PRTG Hosted Monitor
- Step 4: Install a New Remote Probe 110
- Step 5: Approve the New Remote Probe 113

Step 1: Meet the Requirements

To install a remote probe on a target system, make sure that you meet the following requirements.

- The target system runs on at least Windows 7.
- The target system is accessible via remote procedure call (RPC). This is usually the case when your PRTG core server and the target system are located in the same LAN segment. Otherwise, open Windows services.msc on the target system and start the RPC service.
- Programs are allowed to communicate through your Windows Firewall. Open the settings of your firewall and select Allow an app through firewall. Mark the check box for Remote Service Management, and the check box Public in the corresponding line.

- Because the probe initiates the connection, you must ensure that a connection to your PRTG core server from the outside can be established. The process is the same as if you wanted to allow access to the PRTG web server provided by the PRTG core server via port 80 or 443. In most cases, this means that you will require an allow or allow-nat network address translation (NAT) rule that enables the probe to reach the PRTG core server via the Transmission Control Protocol (TCP) port 23560. Then, the probe uses a dynamic port from the high port range (49152 - 65535) for outgoing connections.

  If you need to set a different port, which we do not recommend, see the Knowledge Base: How can I customize ports for core-probe connections used by PRTG?

PRTG Network Monitor and PRTG Hosted Monitor already include a local probe or hosted probe on the PRTG core server. This is why you cannot additionally install a remote probe on your PRTG core server system.

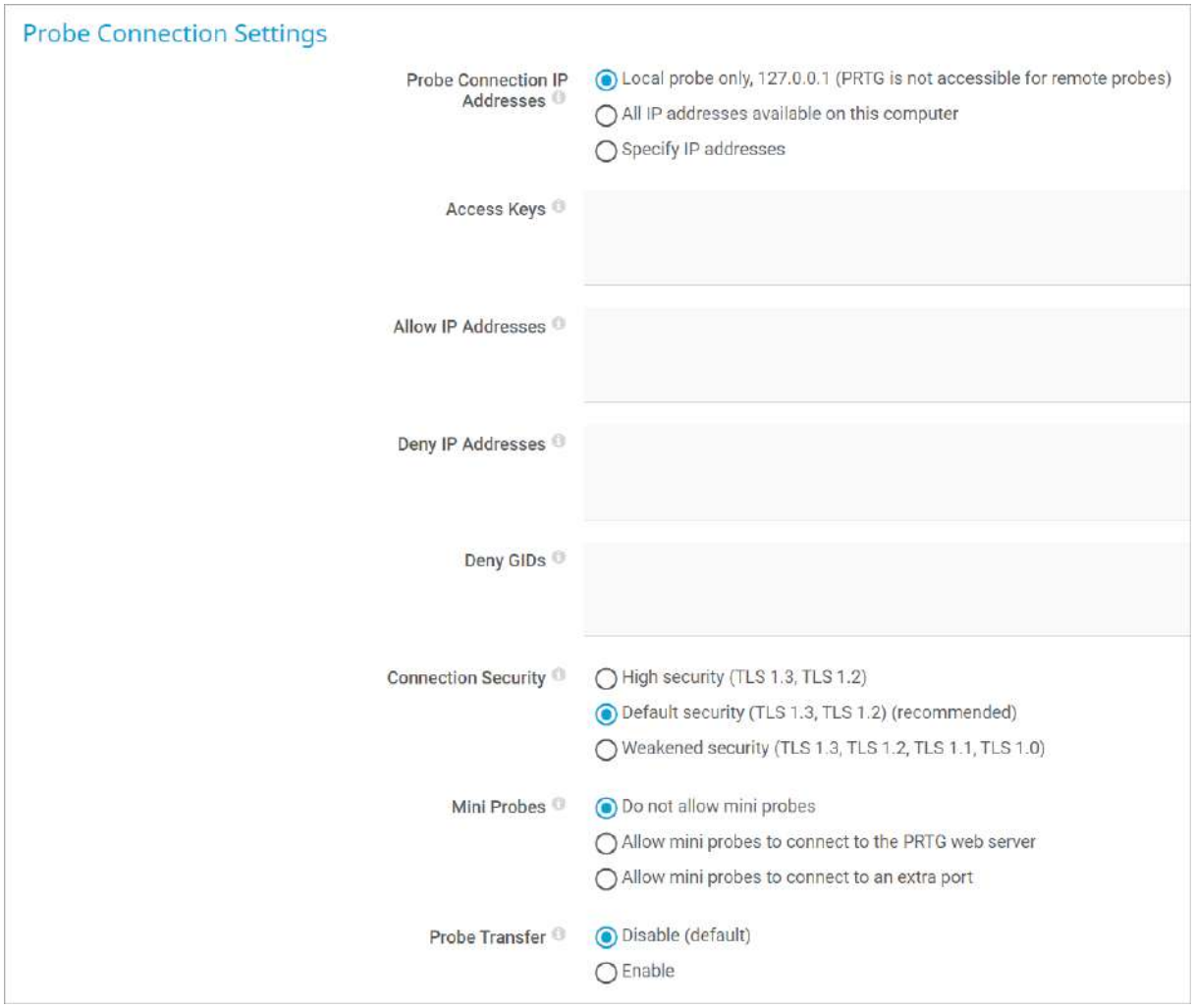
For more information on the requirements for remote probes, see section System Requirements 24.

Step 2: Prepare the PRTG Core Server

If you use PRTG Hosted Monitor, you can start with Step 3: Download the Remote Probe Installer from the PRTG Web Interface 109 right away.

Because your remote probe needs to connect to your PRTG core server, PRTG needs to accept incoming remote probe connections. So, with PRTG Network Monitor, first prepare your PRTG core server before you install the remote probe.

Edit the relevant settings in section Core & Probes 3325. From the main menu in the PRTG web interface 124, select Setup | System Administration | Core & Probes to access the probe settings and go to the Probe Connection Settings.



Probe Connection Settings in System Administration

Step 2.1: Probe Connection IP Addresses

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

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

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

Step 2.2: Allow IP Addresses

In the Allow IP Addresses field, you can enter the IP address of the target system on which you want to install a remote probe. You can also enter the word any. This sets the PRTG core server to accept remote probe connections from any IP address.

ⓘ If you use any, make sure that you only write the word in lower case. Other variations are not valid.

Other settings are not required. For details about the fields for Access Keys, Deny IP Addresses, and Deny GIDs, see section Core & Probes 3327.

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

If you change this setting, PRTG needs to restart the PRTG core server to apply your changes. After you click Save, a dialog box appears that asks you to confirm the restart. Click OK to trigger the restart. During the restart, all users of the PRTG web interface, of PRTG Desktop 3417, or of PRTG Apps for Mobile Network Monitoring 3420 are disconnected and reconnected.

To edit the core–probe connection settings, you can also use the PRTG Administration Tool 3469 on your PRTG core server.

Cluster and Remote Probes Outside the LAN

If you run PRTG as a cluster and you want to run remote probes outside your local network, you must make sure that your cluster nodes and the addresses that they use are reachable from the outside. Check your cluster node settings under Cluster 3356 before you install a remote probe outside your local network. Enter valid Domain Name System (DNS) names or IP addresses for both cluster nodes to reach each other and for remote probes to individually reach all cluster nodes. Remote probes outside your LAN cannot connect to your cluster nodes if they use local addresses.

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

1. Uninstall the remote probe.
2. Update the cluster node settings 3356 with addresses that are reachable from outside your LAN.
3. Restart the PRTG core servers.
4. Install the remote probe again. It then obtains the IP address or DNS name entries that it can reach.

See also section Failover Cluster Configuration 3633, section Remote Probes in a Cluster.

Step 3: Download the Remote Probe Installer from the PRTG Web Interface

1. On the computer on which you want to install a remote probe, log in to the PRTG web interface.
2. From the main menu bar, select Setup | Optional Downloads | Remote Probe Installer.
3. Click Add Remote Probe to start the installation assistant.
   The Add Remote Probe button is also available in the device tree.
4. Wait until the installation is completed. The remote probe then automatically connects to your PRTG core server.
5. In the appearing dialog window, click Prepare and Download to start the download.
6. Save the setup program to your local disk.

In the installation approach with the assistant, PRTG guides you through the installation process. If you Download the Remote Probe Installer directly, you must install the remote probe without the assistant.

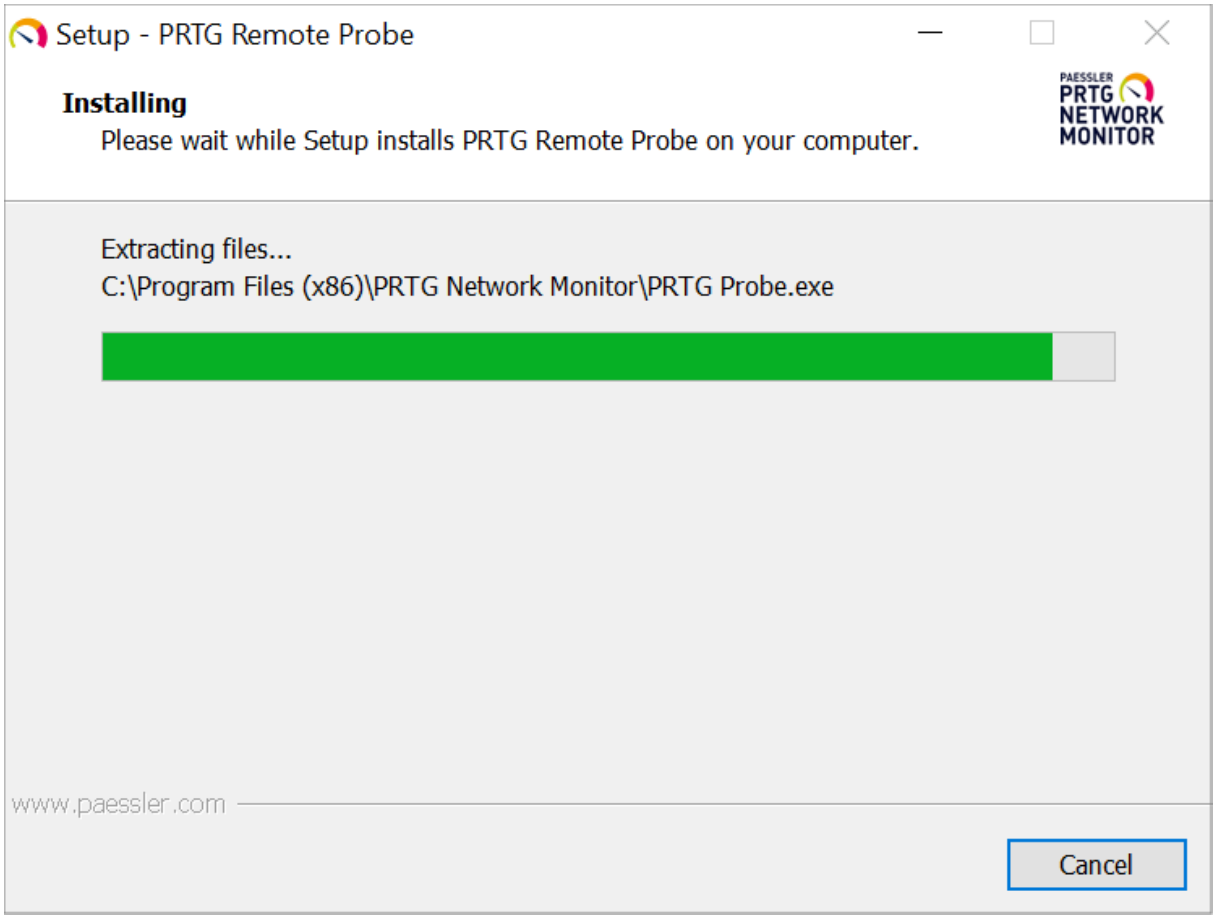
If you connect your remote probe to PRTG Network Monitor, prepare 107 your Probe Connection Settings first.

Add Remote Probe Assistant

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

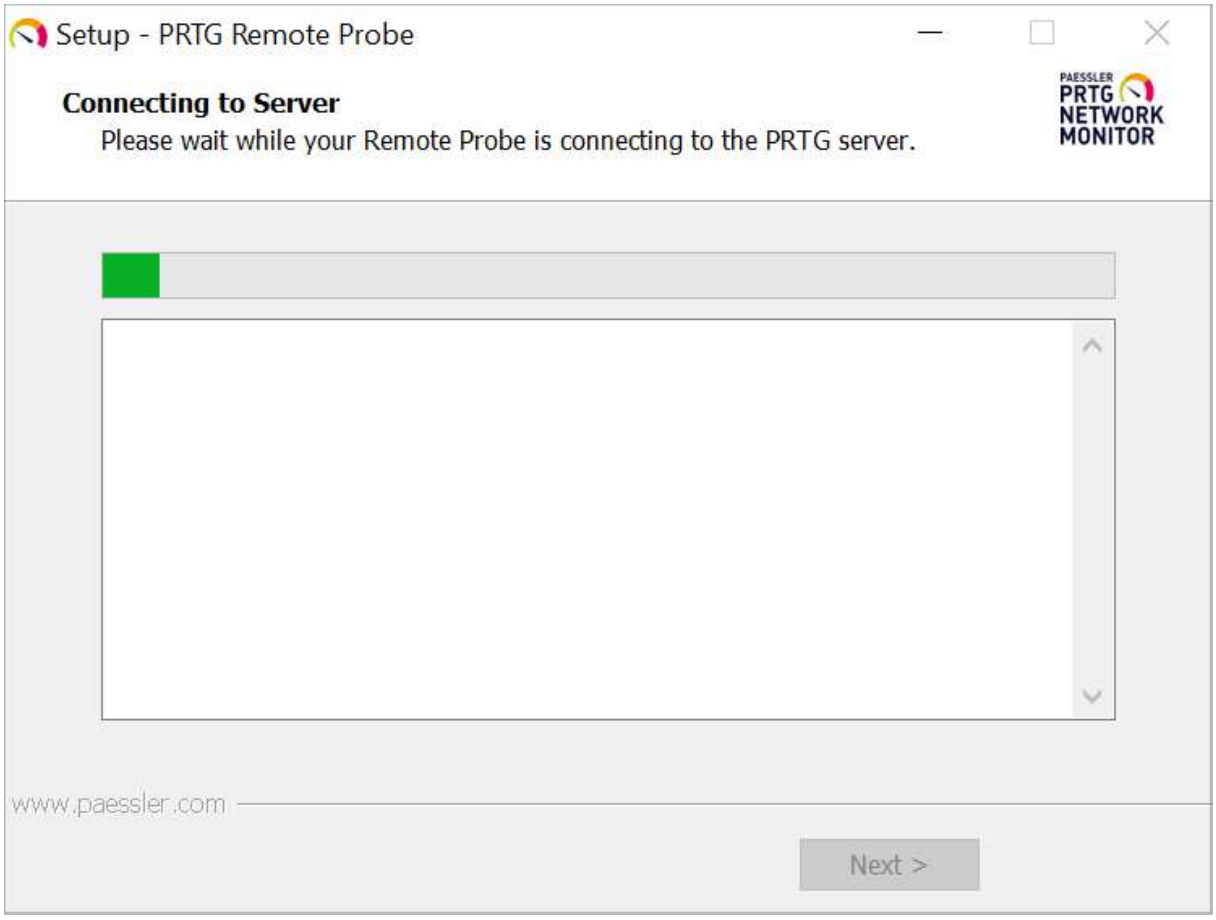
Step 4: Install a New Remote Probe

1. Execute the setup program that you downloaded.
2. Confirm the Windows User Account Control dialog with Yes to allow the installation. The usual software installation wizard guides you through the installation process.
3. Click Install to start the installation process.



Remote Probe Setup Installing

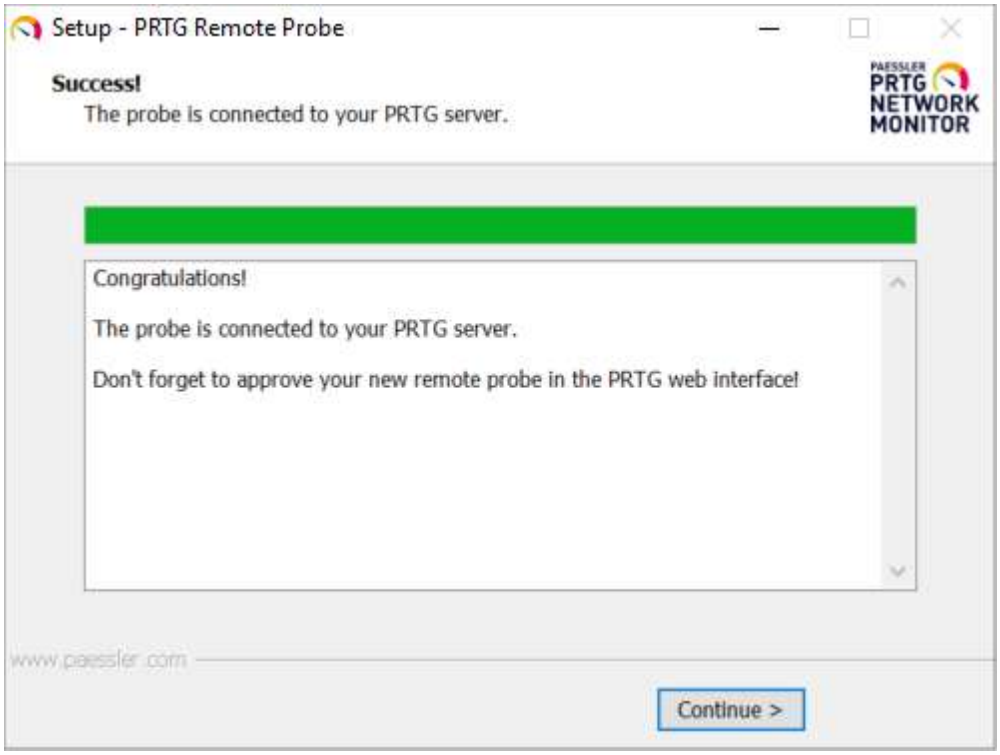
Wait until the installation is complete. The remote probe then automatically connects to your PRTG core server.



Remote Probe Setup Connecting to the PRTG Core Server

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

ⓘ To allow your new remote probe to connect to a PRTG Hosted Monitor instance, PRTG automatically sets the Allow IP Addresses field in Core & Probes 3327 to any. You can also use any for PRTG Network Monitor, but we recommend that you use this setting in intranets only. If any is not an option for you, cancel it in the Allow IP Addresses field and enter the IP address of your remote probe instead.



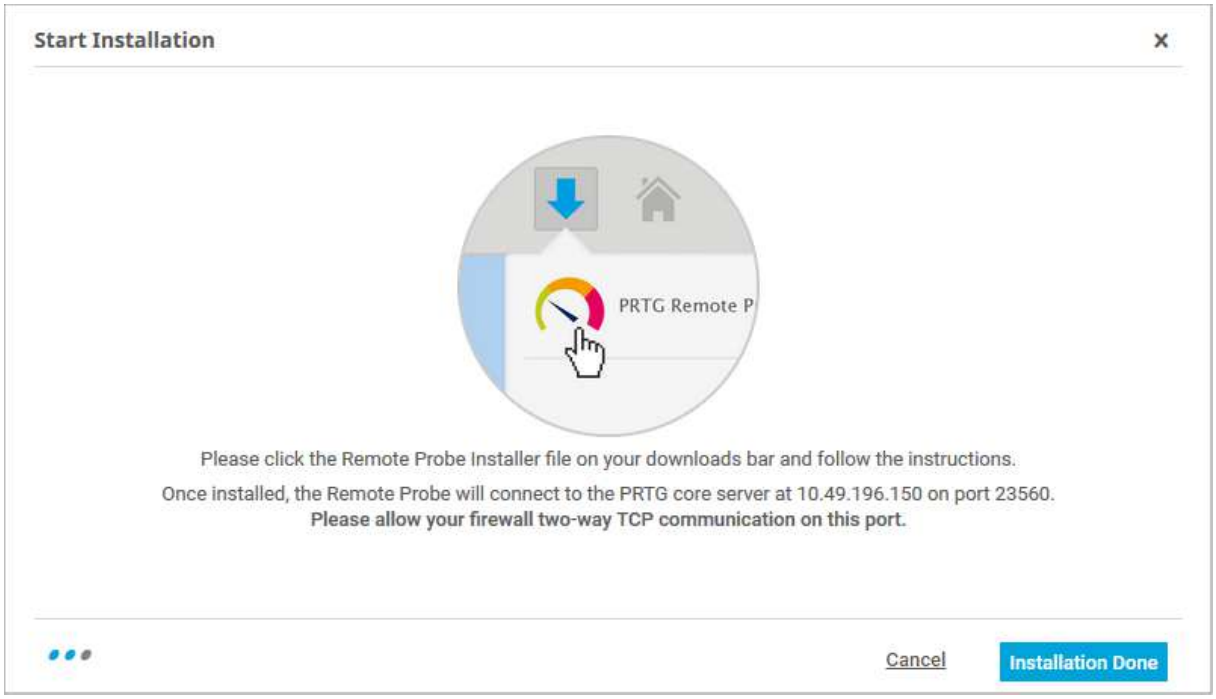
Remote Probe Setup Successful

4. Click Continue to finish the remote probe installation.
5. Click Finish to exit the installation wizard.

The remote probe is now installed on your computer as a Windows service.

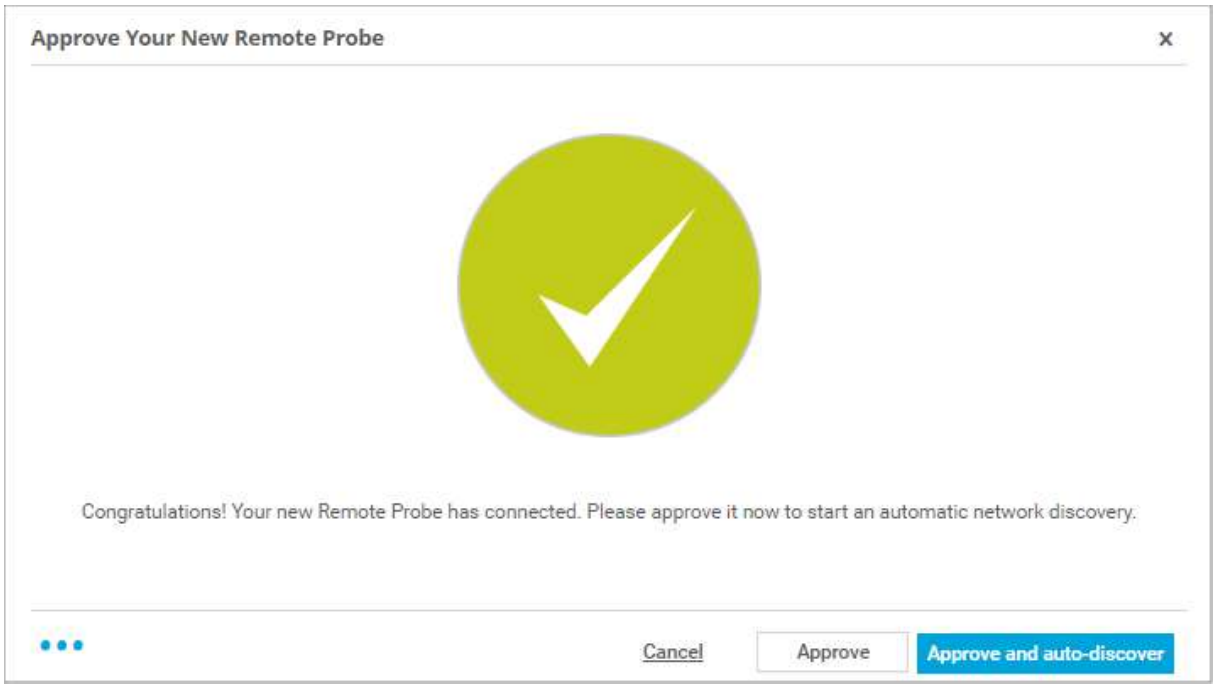
Step 5: Approve the New Remote Probe

In the installation assistant, click Installation Done.



Confirm that Installation is Done

If you successfully installed the remote probe from a PRTG Hosted Monitor installation, you see the following dialog box.



Approve Remote Probe for PRTG Hosted Monitor

Click Approve and auto-discover to include the new remote probe and network in your device tree and to start the auto-discovery 264. It discovers devices and automatically creates suitable sensors. Optionally, click Approve to only approve the remote probe without the auto-discovery. The remote probe appears in your device tree.

For unwanted remote probe connections, click Cancel. A new window appears in the lower-right corner.

Deny Remote Probe

Click Deny to deny the new remote probe.

If you deny or remove a remote probe, PRTG automatically adds the global ID (GID) of this device to the Deny GIDs list in Core & Probes 3325. PRTG automatically denies future remote probe connections from this device.

If you deny the remote probe in the device tree, it does not uninstall the remote probe, but only denies access to the PRTG core server. The remote probe continues to run on the target system until you uninstall it manually.

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

You do not need to approve remote probes after updates.

When a new remote probe connects to the PRTG core server for the first time, you receive a new ToDo ticket.

Debugging Remote Probe Connection Issues

If you have issues with the connection between the PRTG core server and remote probe, make sure that you meet the following requirements:

- Recheck if you fulfilled all the requirements as described in step 1 106 of this section like the Windows Firewall settings.
- The IP address of the computer on which you want to install a remote probe is not listed in the Deny IP Addresses field in Core & Probes 3325.
- You can also take a look at the log files of the remote probe. The probe process writes log files with a file name in the format PRTG Probe Log (x).log. Open the one with the most recent date.

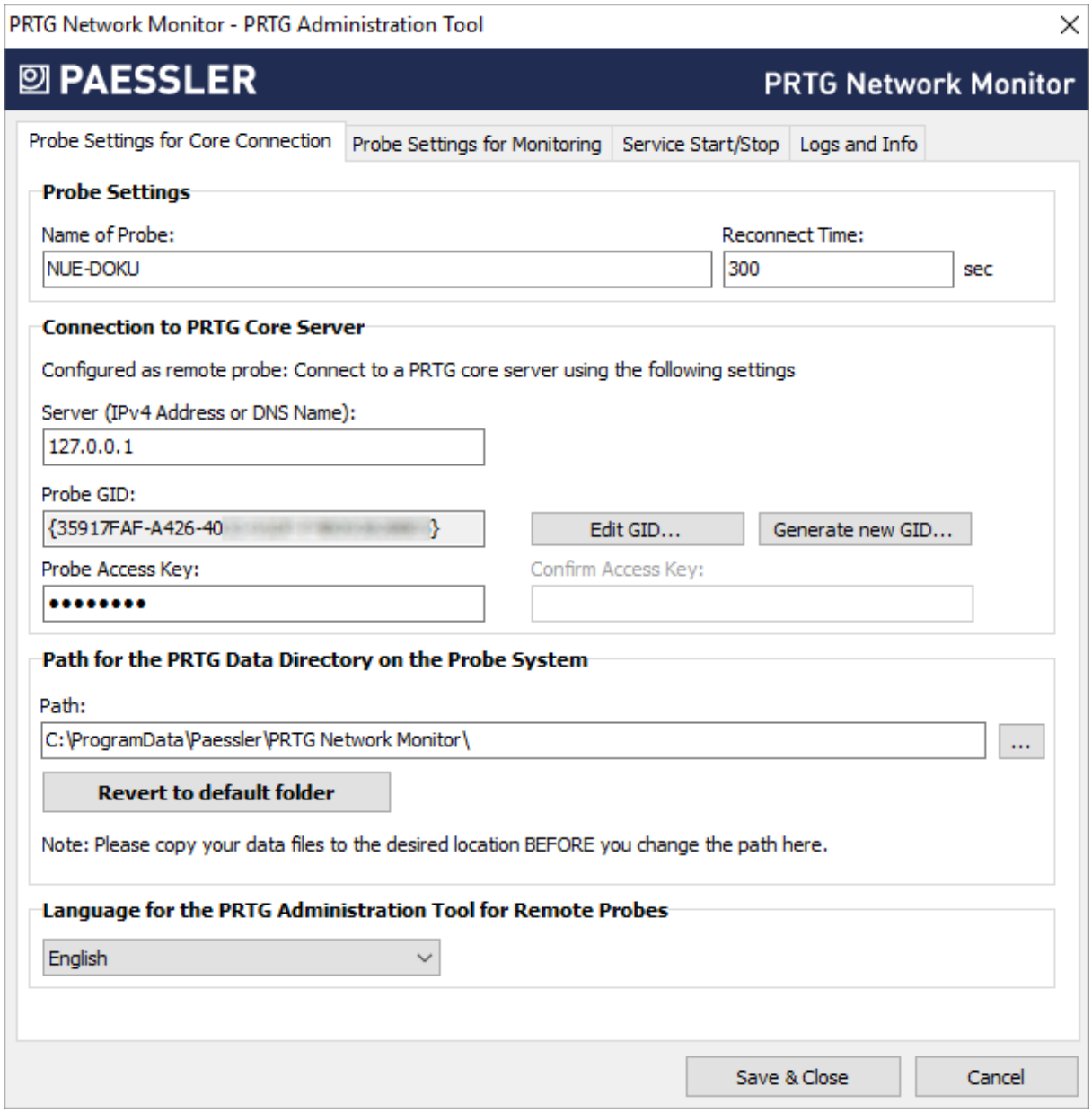
For a correct connection, the log should look similar to this:

```
11/6/2017 1:21:58 PM PRTG Probe V17.4.36.3253
11/6/2017 1:21:58 PM System time zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome,
Stockholm, Vienna
11/6/2017 1:21:58 PM libeay32.dll=1.0.2.11
11/6/2017 1:21:58 PM ssleay32.dll=1.0.2.11
11/6/2017 1:21:58 PM PRTG Probe "example-DNS" starting on "example-
DNS" (GID={AAAA1111-22BB-33CC-DD44-EEEEEE555555})
11/6/2017 1:21:58 PM Memory Manager: NexusMM4
11/6/2017 1:21:58 PM OS: Microsoft Windows 10 Enterprise (10.0 Build 15063), 4 CPUs
(Quad x64 Model 78 Step 3), code page "Windows-1252", on "NVME SAMSUNG MZFLV256"
11/6/2017 1:21:58 PM Data Path: C:\ProgramData\Paessler\PRTG Network Monitor\
11/6/2017 1:21:58 PM System Path: C:\Program Files (x86)\PRTG Network Monitor\
11/6/2017 1:21:58 PM Local IP: 0.0.0.0
11/6/2017 1:21:58 PM Core Server IP: example-DNS.exampledomain.com
11/6/2017 1:21:58 PM Core Server Port: 23560
11/6/2017 1:21:58 PM SSL Enabled
11/6/2017 1:21:58 PM Probe GID: {AAAA1111-22BB-33CC-DD44-EEEEEE555555}
[...]
11/6/2017 1:21:58 PM Start Connection
11/6/2017 1:21:58 PM Start Done
11/6/2017 1:21:58 PM (14608):Initializing WMIConnectionPool
11/6/2017 1:21:58 PM (14608):WMIConnectionPool maximum number of concurrent
establishings is set to: 20
11/6/2017 1:22:03 PM Connect from to example-DNS.exampledomain.com:23560
11/6/2017 1:22:03 PM TCP connected from 10.49.12.51:55199 to example-
DNS.exampledomain.com:23560
11/6/2017 1:22:03 PM State changed to connected (example-DNS.exampledomain.com:23560)
11/6/2017 1:22:03 PM Reconnect
11/6/2017 1:22:04 PM Connected
11/6/2017 1:22:10 PM Send Login
11/6/2017 1:22:10 PM Local: 11/6/2017 1:22:10 PM UTC: 11/6/2017 12:22:10 PM
11/6/2017 1:22:10 PM MarkUnused
11/6/2017 1:22:10 PM Login OK: Welcome to PRTG
```

If the connection fails, for example because of an incorrect Access Key, or because of incorrect IP address settings (see step 2 107), you see:

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

If you need to adjust any settings for the connection to the PRTG core server, use the PRTG Administration Tool 3494 on the remote probe system.



Remote Probe Settings in PRTG Administration Tool

Under Connection to PRTG Core Server, you can then edit the following settings:

- Server (IPv4 Address or DNS Name): Enter the IP address or Domain Name System (DNS) name of the PRTG core server that the remote probe is to connect to. If you use network address translation (NAT) rules, you must enter the IP address that is externally visible, because the remote probe connects from outside your network.
- Access Key and Confirm Access Key: Enter the access key that the remote probe is to send to the PRTG core server. You must define this access key on the PRTG core server in Core & Probes 3325. Make sure that the access keys match.

Click Save & Close to confirm your settings and to (re)start the PRTG probe service.

For more information about these settings, see section PRTG Administration Tool 3494.

More

KNOWLEDGE BASE

How can I customize ports for core-probe connections used by PRTG?

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

I cannot open the PRTG web interface via the desktop shortcut anymore. What can I do?

- https://kb.paessler.com/en/topic/89024

PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- https://www.paessler.com/support/how-to/firewall

How to install a PRTG remote probe in 4 steps

- https://www.paessler.com/support/how-to/remote-probe-installation

4.8 Uninstall PRTG Products

Whether you uninstall an entire PRTG installation or a remote probe installation, take the following steps. Use the Windows uninstall routines to remove the software from your system.

Step 1

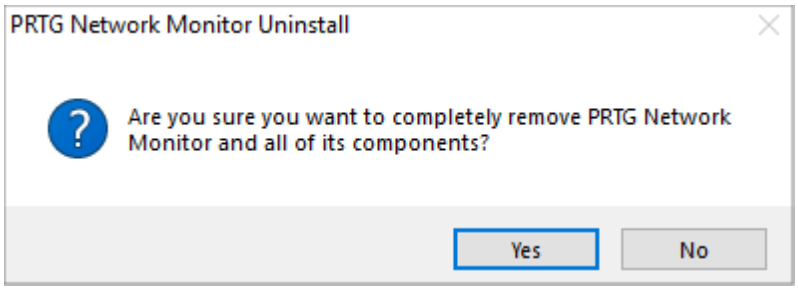
From the Windows Start menu, run Uninstall PRTG Network Monitor or open your Windows Control Panel and select the desired entry in the Programs and Features section. To uninstall a remote probe, only the second option applies. Depending on the installed products, not all uninstall programs are available.

Step 2

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

Step 3

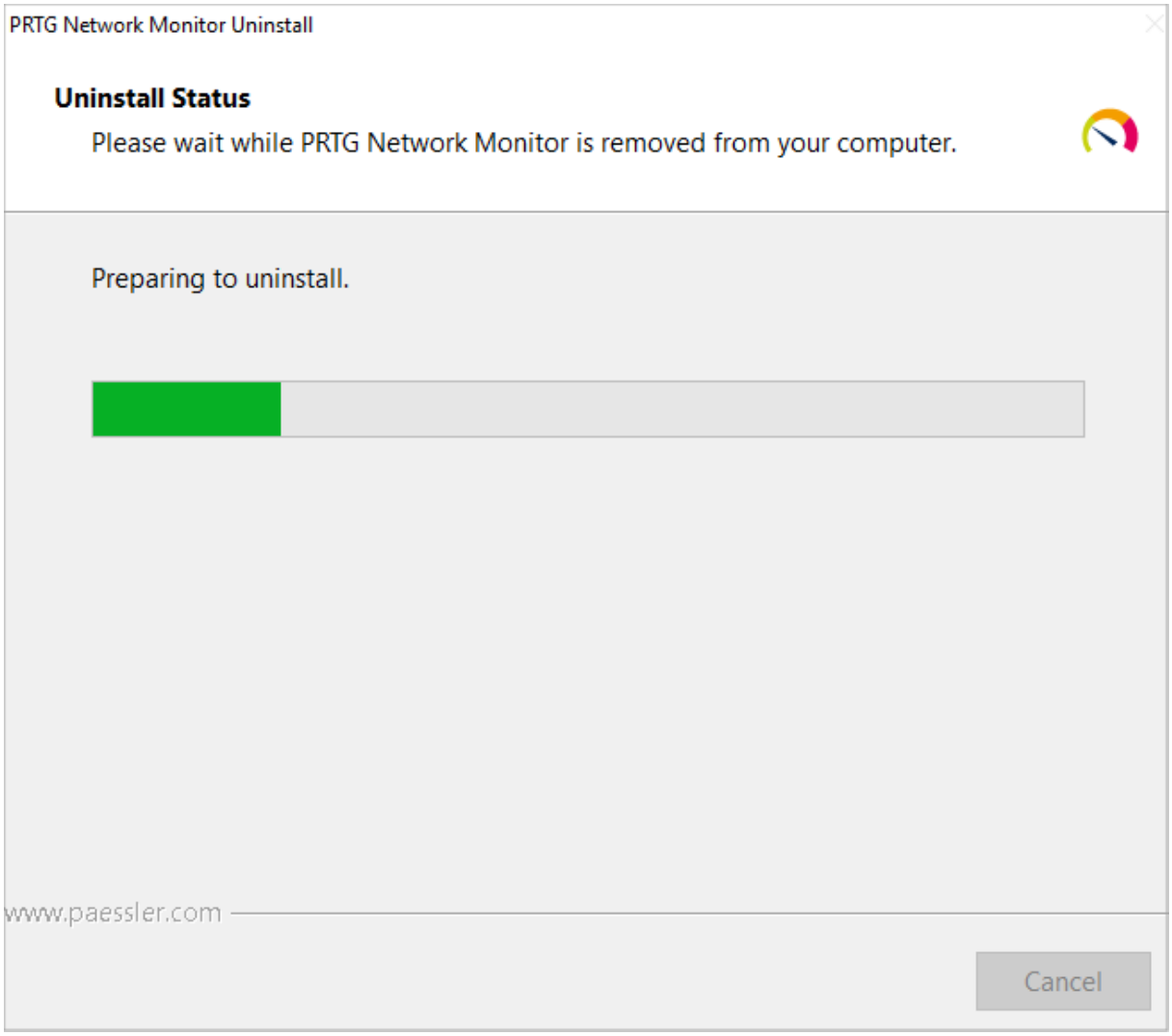
Confirm the removal of the software with Yes.



Uninstall PRTG Network Monitor Step 1

Step 4

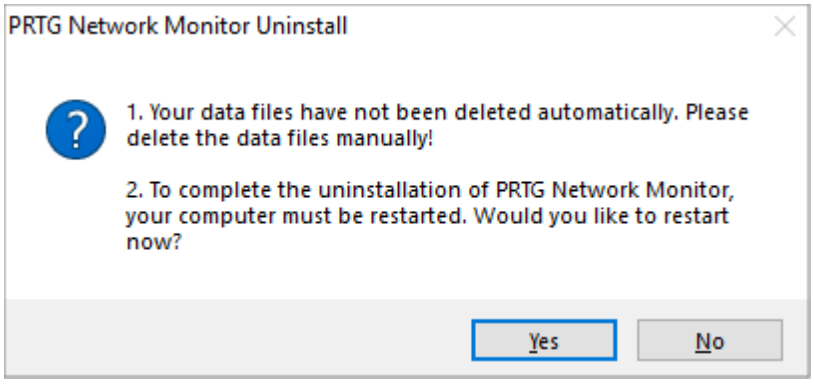
Wait while the software is removed.



Uninstall PRTG Netw ork Monitor Step 2

Step 5

Confirm a system restart with Yes.



Uninstall PRTG Netw ork Monitor Step 3

Step 6

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

For more information, see section Data Storage 3636.

Step 7

During the installation of PRTG, a component called Npcap is also installed on your system. After you uninstall PRTG, you need to manually uninstall this feature. To do so, open your Windows Control Panel and select Npcap 0.9983 in the Programs and Features section. Click Uninstall to remove this feature from your Windows system.

If you updated to PRTG 19.2.50, you also need to manually uninstall the Npcap loopback adapter. For more information, see the Knowledge Base: I have issues with additional services after updating to PRTG 19.2.50. What can I do?

More

KNOWLEDGE BASE

I have issues with additional services after updating to PRTG 19.2.50. What can I do?

- https://kb.paessler.com/en/topic/86103

Can we remotely and silently uninstall a remote probe?

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

Part 5
Understanding Basic Concepts

5 Understanding Basic Concepts

There are a number of basic concepts that are essential for understanding the functionality of PRTG. This includes, for example, the underlying architecture of the monitoring system, the hierarchy of objects, the inheritance of settings, the access rights management, and notifications.

In this section:

- Architecture and User Interfaces 124
- Failover Cluster 128
- Object Hierarchy 131
- Inheritance of Settings 135
- Tags 137
- Dependencies 139
- Scheduling 140
- Notifying 141
- Access Rights Management 144
- Data Reporting 148
- IPv6 Support 149

5.1 Architecture and User Interfaces

In this section, you can find an overview of the components of PRTG and how it works.

Overview

You can classify the components of PRTG into three main categories: system parts, user interfaces, and basic system administration tools.

Category	Components
System Parts	PRTG core server 125 This is the central part of a PRTG installation. The PRTG core server includes the data storage, the web server, the report engine, the notification system, and more. The PRTG core server is configured as a Windows service that permanently runs. Probes 125 This is the part of PRTG that performs the actual monitoring. There are local probes, remote probes, and cluster probes in PRTG Network Monitor, and there are hosted probes and remote probes in PRTG Hosted Monitor. Probes forward all monitoring data to the central PRTG core server. Probes are configured as Windows services that permanently run. We assume that all systems on which the PRTG core server with the local probe or any remote probes run are secure. It is every system administrator's responsibility to make sure that only authorized persons can access these systems. For this reason, we highly recommend that you use dedicated machines for your PRTG system parts.
User Interfaces	PRTG web interface With the Asynchronous JavaScript and XML (AJAX) based PRTG web interface, you can configure devices and sensors, review monitoring results, and configure the system administration and user management. PRTG Desktop 3417 PRTG Desktop is a cross-platform application that you can use as an alternative interface for fast access to data and monitoring management. With PRTG Desktop, you can connect to several independent PRTG core servers or PRTG Hosted Monitor instances to display their data and centrally manage your monitoring. PRTG apps for mobile network monitoring 3420 With the PRTG apps for iOS and Android, you can monitor your network on the go and receive push notifications in case of alerts.
System Administration Tools	PRTG Administration Tool on PRTG Core Server Systems 3469 With the PRTG Administration Tool on the PRTG core server system, you can configure basic PRTG core server settings in PRTG Network Monitor such as the PRTG System Administrator user login, web server IP addresses and the web server port, probe connection settings, the cluster mode, the system language, and more.

Category	Components
	PRTG Administration Tool on Remote Probe Systems 3494 With the PRTG Administration Tool on the remote probe system, you can configure basic remote probe settings such as the name of the remote probe, IP address and server connection settings, and more.

PRTG Core Server

The PRTG core server is the heart of PRTG. It performs the following tasks:

- Configuration management for target devices (for example, servers, workstations, printers, switches, routers, or virtual machines (VM))
- Management and configuration of connected probes
- Cluster management
- Database for monitoring results
- Notification management including a mail server for email delivery
- Report generation and scheduling
- User account management
- Data purging (for example, deleting data that is older than 365 days)
- Web server and application programming interface (API) server

In a cluster 128, the master node is responsible for all of these tasks.

The built-in and secure web server, for which you require no additional Microsoft Internet Information Services (IIS) or Apache, supports HTTP as well as HTTPS (secured with Secure Sockets Layer (SSL)/Transport Layer Security (TLS)). It serves the PRTG web interface when you access it via a browser and also answers PRTG API calls.

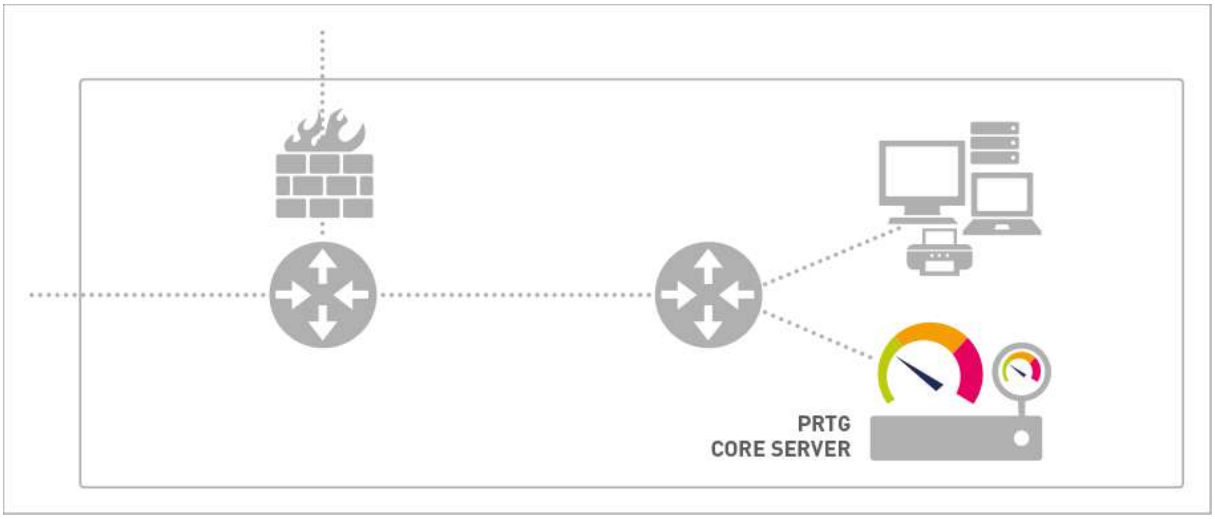
The PRTG core server is configured as a Windows service that permanently runs. A logged-in user is not required.

Probes

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

For PRTG Network Monitor, there is always a local probe that runs on the PRTG core server system.

For PRTG Hosted Monitor instances, there is always a hosted probe that runs on the PRTG core server system that Paessler hosts for you.



PRTG Core Server and Local Probe That Monitors a LAN

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

ⓘ The probes are configured as a Windows service that permanently runs. A logged-in user is not required.

Probe Type	Description
Local probe	During the installation, PRTG automatically creates the local probe. In a single-probe installation, which is the default setup, the local probe performs all monitoring. For PRTG Network Monitor, the PRTG core server with the local probe inside the corporate LAN can monitor services and servers in the entire LAN.
Hosted probe	When you create a PRTG Hosted Monitor instance, the system automatically creates the hosted probe. The hosted probe shows monitoring values of the hosted instance and can monitor devices, servers, and services that are publicly available in the internet like websites.
Remote probes	You can create additional remote probes to monitor multiple locations, to monitor a LAN with PRTG Hosted Monitor, or for several other scenarios. Remote probes use SSL/TLS-secured connections to the PRTG core server. With remote probes, you can securely monitor services and systems inside remote networks that are not publicly available or that are secured by firewalls. For more information, see section Add Remote Probe 3619. For more information, see the video tutorial: Distributed monitoring with PRTG.

Probe Type	Description
Cluster probes	In a cluster, a cluster probe runs on all cluster nodes. All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails.
Mini probes	Mini probes let you create small probes on any device, not only on Windows systems. For more information, see section Mini Probe API 3576.

System Health Monitoring

PRTG automatically monitors the system health of the PRTG core server and of each probe to discover overload situations that might distort monitoring results. To monitor the status of the probe system, PRTG automatically creates the Core Health and Probe Health sensor, the System Health sensor, the Cluster Health sensor, some disk free and bandwidth sensors for all installed network cards, as well as a Common SaaS sensor that checks the availability of widely used software as a service (SaaS) providers.

We recommend that you keep these sensors. However, you can remove all of them except for the health sensors.

The health sensors measure various internal system parameters of the probe system hardware and the probe's internal processes and compute the results. Investigate frequent values below 100%.

More

PAESSLER WEBSITE

Getting started with PRTG

- https://www.paessler.com/support/getting-started

How to connect PRTG through a firewall in 4 steps

- https://www.paessler.com/support/how-to/firewall

VIDEO TUTORIAL

Distributed monitoring with PRTG

- https://www.paessler.com/support/videos-and-webinars/videos/distributed_monitoring

What is a sensor?

- https://www.paessler.com/support/videos-and-webinars/videos/what-is-a-sensor

5.2 Failover Cluster

A cluster consists of two or more PRTG core servers that work together to form a high-availability monitoring system.

This feature is not available in PRTG Hosted Monitor.

Cluster Concept

A cluster consists of at least two cluster nodes: one master node and one or more failover nodes, where up to four failover nodes are possible. Each cluster node is a full PRTG core server installation that can perform all of the monitoring and alerting on its own.

Cluster with Two Cluster Nodes

See the following table for more information on how a cluster works:

Feature	Description
Connection and communication	Cluster nodes are connected to each other with two TCP/IP connections. They communicate in both directions and a single cluster node only needs to connect to one other cluster node to integrate itself into the cluster.
Object configuration	During normal operation, you configure devices, sensors, and all other monitoring objects on the master node. The master node automatically distributes the configuration among all other cluster nodes in real time.
Fail-safe monitoring	All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails. If the master node fails, one of the failover nodes takes over and controls the cluster until the master node is back. This ensures continuous data collection.

Feature	Description
Active-active mode	A cluster works in active-active mode. This means that all cluster nodes permanently monitor the network according to the common configuration that they receive from the master node. Each cluster node stores the results in its own database. PRTG also distributes the storage of monitoring results among the cluster.
PRTG updates	You only need to install PRTG updates on one cluster node. This cluster node automatically deploys the new version to all other cluster nodes.
Notification handling	If one or more cluster nodes discover downtime or threshold breaches, only one installation, either the primary master node or the failover master node, sends out notifications, for example, via email, SMS text message, or push message. Because of this, there is no notification flood from all cluster nodes in case of failures.
Data gaps	During the outage of a cluster node, it cannot collect monitoring data. The data of this single cluster node shows gaps. However, monitoring data for the time of the outage is still available on the other cluster nodes. ⓘ There is no functionality to fill these gaps with the data of other cluster nodes.
Monitoring results review	Because the monitoring configuration is centrally managed, you can only change it on the primary master node. However, you can review the monitoring results of any of the failover nodes in read-only mode if you log in to the PRTG web interface.
Remote probes	If you use remote probes in a cluster 3633, each remote probe connects to each cluster node and sends the data to all cluster nodes. You can define the Cluster Connectivity of each remote probe in its settings 515.

Performance Considerations for Clusters

Monitoring traffic and load on the network is multiplied by the number of used cluster nodes. Furthermore, the devices on the cluster probe are monitored by all cluster nodes, so the monitoring load increases on these devices as well.

For most usage scenarios, this does not pose a problem, but always keep in mind the system requirements 26. As a rule of thumb, each additional cluster node means that you need to divide the number of sensors that you can use by two.

ⓘ PRTG does not officially support more than 5,000 sensors per cluster. Contact the Paessler Presales team if you exceed this limit. For possible alternatives to a cluster, see the Knowledge Base: Are there alternatives to the cluster when running a large installation?

Cluster Setup

For more information, see section Failover Cluster Configuration 3631.

More

KNOWLEDGE BASE

What is the clustering feature in PRTG?

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

In which web interface do I log in to if the master node fails?

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

What are the bandwidth requirements for running a cluster?

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

Are there alternatives to the cluster when running a large installation?

- https://kb.paessler.com/en/topic/75474

PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

- https://www.paessler.com/support/how-to/firewall

VIDEO TUTORIAL

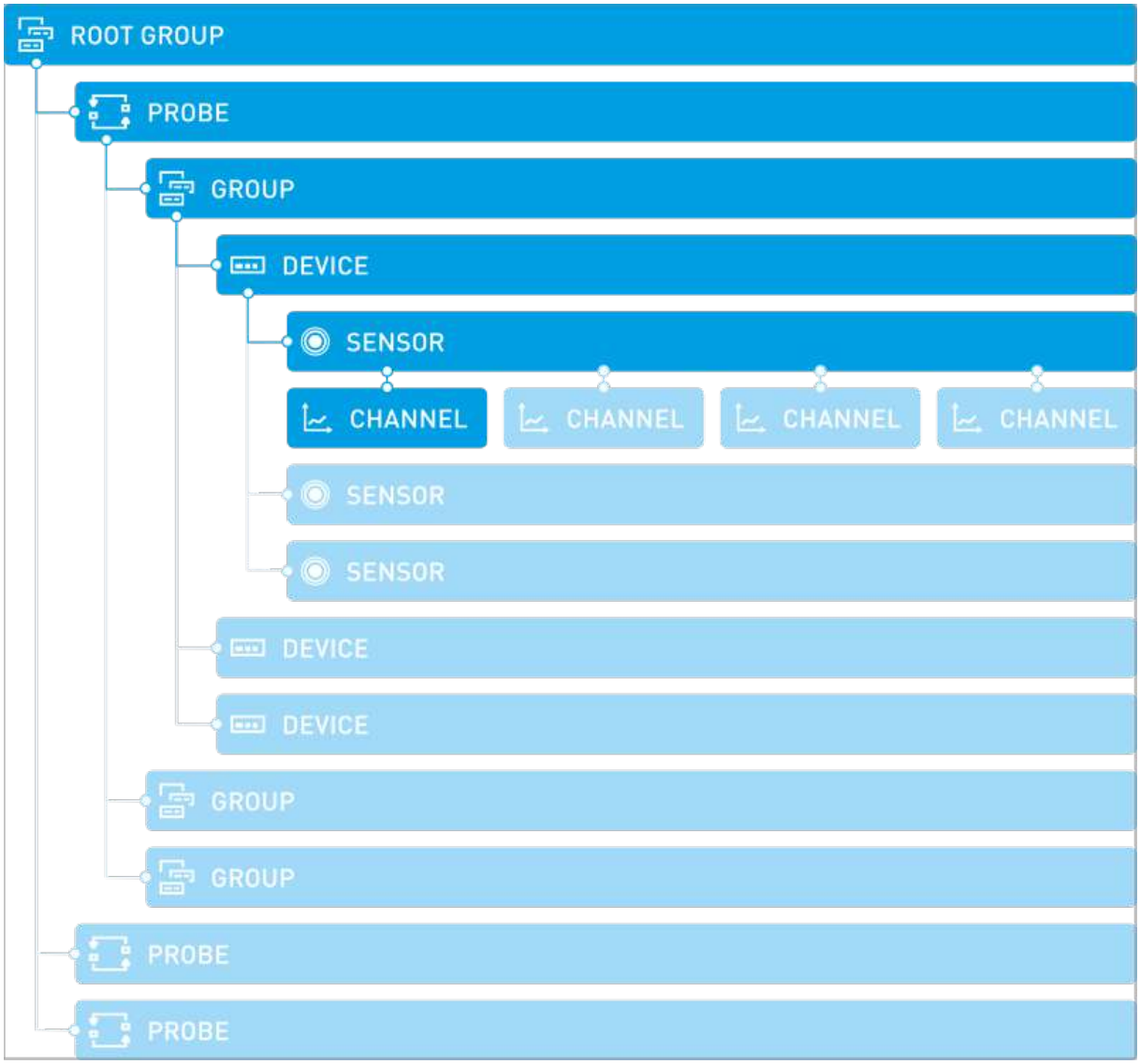
How to set up a PRTG cluster

- https://www.paessler.com/support/videos-and-webinars/videos/how-to-set-up-a-cluster

5.3 Object Hierarchy

PRTG arranges all objects in the monitoring configuration in a tree-like hierarchy. You can arrange the objects in groups that monitor similar devices, services, or particular locations. You can also use this hierarchical order to define common settings for larger groups of objects. The settings of the root group, for example, apply to all other objects underneath in the object hierarchy by default.

For more information, see section Inheritance of Settings 135.



Object Hierarchy in PRTG

Root Group

The root group is the topmost instance in PRTG. It contains all other objects in your setup. We recommend that you adjust all default settings for the root group 419. This is because all other objects in the device tree inherit 135 these standard settings by default so that you do not need to set up the same configuration for each object anew.

Probe

Each group (except the root group) is part of a probe. This is where the actual monitoring takes place. All objects that you add to a probe are monitored via that probe. In PRTG Network Monitor, every PRTG core server installation automatically installs the local probe. In PRTG Hosted Monitor, every instance has the hosted probe.

In a failover cluster 128, there is an additional cluster probe that runs on all cluster nodes. All devices that you create on the cluster probe are monitored by all cluster nodes, so data from different perspectives is available and monitoring continues even if one of the cluster nodes fails.

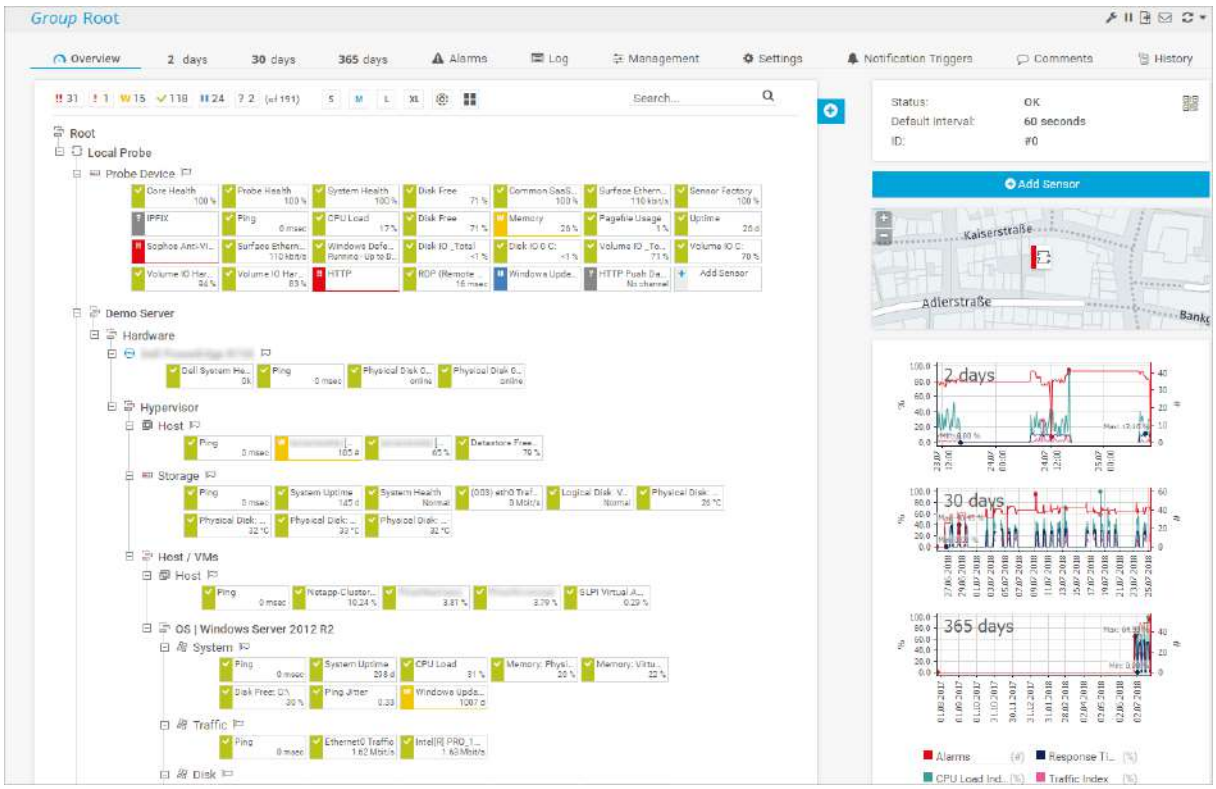
You can add additional probes and remote probes to your configuration to also monitor remote devices from outside your network.

For more information, see section Add Remote Probe 3619.

Group

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

Here you can see a sample configuration of a device tree with the local probe, several groups, devices, and their sensors:



Object Hierarchy in the Device Tree

Device

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

- Web or file servers
- Client computers (Windows, Linux, or macOS)
- Routers or network switches
- Almost every device in your network that has its own IP address

You can add devices with the same IP address or Domain Name System (DNS) name multiple times. This way, you can get a more detailed overview when you use a large number of sensors or you can use different device settings for different groups of sensors. The sensors on all of these devices then query the same real hardware device in your network.

PRTG additionally adds the probe device to the local probe. This is an internal system device with several sensors. It has access to the probe system and monitors the system's health parameters.

PRTG automatically analyzes the devices that you add and recommends appropriate sensors on the Overview tab of the device. To create recommended sensors, click Add These Sensors in the Recommended Sensors table.

For more information about the Overview tab, see the Knowledge Base: What options do I have to review my monitoring data in detail?

You can turn off the sensor recommendation in the system administration settings under Monitoring 3312.

Sensor

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

- A network service like Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), or HTTP
- The traffic on a network switch
- The CPU load of a device
- The memory usage of a device
- The traffic on one network card
- A NetFlow device
- The system health of a device
- And much more

For more information, see the video tutorial: What is a sensor?

Channel

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

- Downtime and uptime of a device
- Traffic in, Traffic out, or Traffic sum of a bandwidth device (for example, a router)
- Mail traffic of a NetFlow device
- CPU load of a device
- Loading time, Download bandwidth, or Time to first byte of a web page
- Response time of a ping request to a device
- And much more

More

VIDEO TUTORIAL

What is a sensor?

- https://www.paessler.com/support/videos-and-webinars/videos/what-is-a-sensor

5.4 Inheritance of Settings

The hierarchically structured 131 device tree organizes the devices in your network. This object hierarchy is the basis for the inheritance of settings. Objects in the device tree can inherit their settings from a higher level. For example, you can change the scanning interval of all sensors by editing the interval setting of the root group (if you define no other setting underneath in the object hierarchy).

Inheritance to Child Objects

You can override the inheritance of settings to child objects at any level of the object hierarchy if you set a different value for a specific probe, group, device, or sensor. All objects underneath inherit these new settings. Object settings from higher levels do not inherit the new settings.

Settings that are inherited to all objects include:

- Scanning intervals
- Notification triggers 3133
- Credentials for different systems
- Compatibility settings for specific sensor types
- Channel and unit configurations
- Access rights 144
- Tags 137
- Paused status 179: If an object is paused by the user or by a schedule, PRTG sets all sensors on this object to the Paused status as well

ⓘ There is one exception for devices and sensors. Sensors always inherit the IP Address/DNS Name of a device and the compatibility settings. You cannot change these settings at sensor level.

Here you can see the Credentials for Windows Systems setting that the object inherits from the parent:

Inherited Credentials for Windows Systems

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

Credentials for Windows Systems

Click Save for your settings to take effect. If you click after you enter your settings, the object inherits the parent object's settings again and your object-specific settings do not take effect.

Default Settings in Root Group

For all settings except passwords, PRTG already includes a set of default values. The following settings, for example, are inherited by all sensors from the root group:

- A default scanning interval of one minute
- SNMP v1 with the community string set to public (this is the default setting for most devices)
- The dependency type Use parent
- And more

Before you set up your monitoring, we recommend that you review the root group settings and set the default values to suit your setup. This includes the credentials for the different systems in your network that you want to monitor (Windows, Linux, virtual servers, different vendors, and more).

For more information, see section Root Group Settings 419.

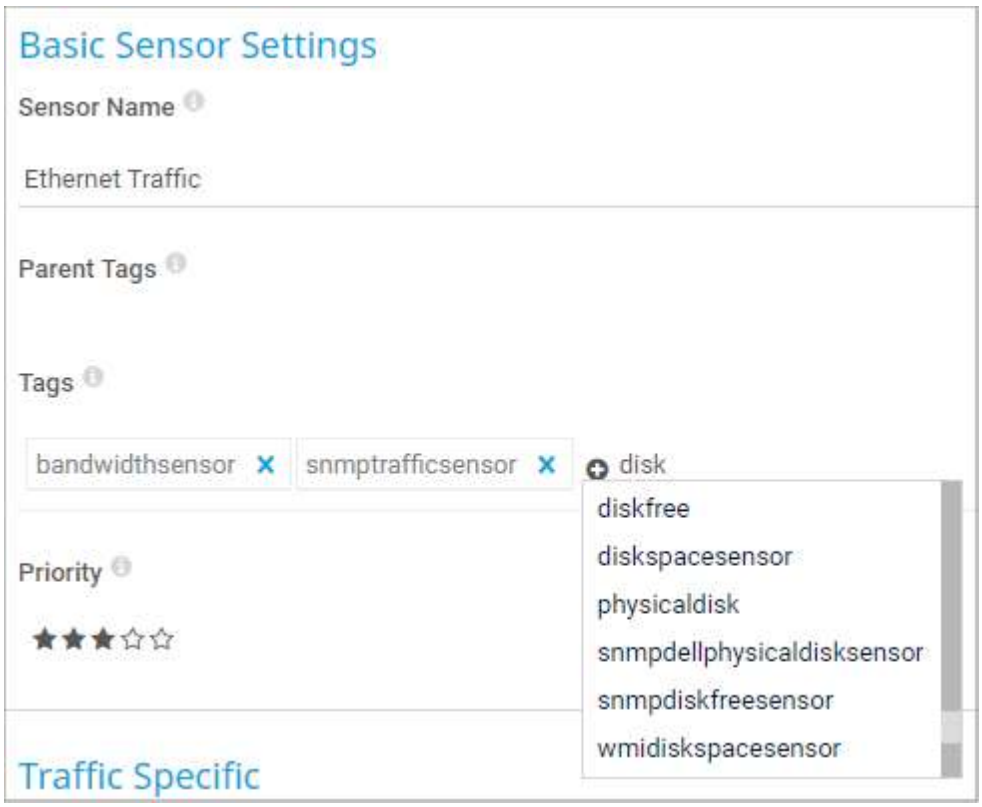
Inheritance of Notification Triggers

If you add notification triggers at probe, group, or device level, these are also inherited to all sensors underneath in the object hierarchy unless you manually disable the inheritance.

For more information, see section Notification Triggers Settings 3133.

5.5 Tags

For every object in your setup, you can define tags in the object settings 198 to additionally categorize these objects. Although some tags are predefined when you add objects 267, you can add further tags. For example, you can mark all bandwidth sensors that are especially important for you with the tag bandwidthimportant.



View and Edit Tags in Basic Sensor Settings

To confirm a tag, use the Enter key, the Spacebar key, or a comma.

ⓘ Use the multi-edit 3158 feature to simultaneously change tags for several objects.

ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>).

ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added.

Inheritance of Tags

Tags in object settings are automatically inherited 135 by all other objects underneath in the object hierarchy 131. You can view inherited tags in section Parent Tags in the settings of a sensor, device, or group.

For example, a device with the tag netflow automatically passes on this tag to all sensors that you add to the device. This is useful, for example, if you include sensors by tag in reports settings 3204. PRTG adds all sensors with the tag netflow to the report so that you do not need to manually tag every single sensor.

You cannot disable the inheritance of tags.

Filter by Tags

You can use one or more tags to filter table lists 216 for specific objects, or to add sensors to libraries 3176 and reports 3192.

When you filter by tags, you can also use the plus sign (+) or the minus sign (-) to categorize tags as must have or must not have.

- Use a tag with a leading + to specify that objects with this tag must be included.
- Use a tag with a leading – to specify that objects with this tag must not be included.
- Use tags without a leading plus or minus sign to specify that objects need to have at least one of these tags to be included.

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

Examples

Here are some examples that show how to filter by tags:

- If you enter –netflow, the table list, library, or report includes all objects that do not have this tag. With the tags +netflow or netflow, you filter for objects that have this tag.
- If you enter +netflow –bandwidthimportant, the table list, library, or report includes all objects that have the tag 'netflow', but excludes all objects that have the tag 'bandwidthimportant'.
- If you enter netflow bandwidthimportant, the table list, library, or report includes all objects that have either the tag 'netflow' or the tag 'bandwidthimportant' or both tags.

Tag Display Limits

For performance reasons, PRTG has a display limit of 1,000 tags when you select Sensors | By Tag in the main menu bar 251. If you have more than 1,000 tags, PRTG shows no tags here. You can, however, still use tags for filters and searches, for example.

5.6 Dependencies

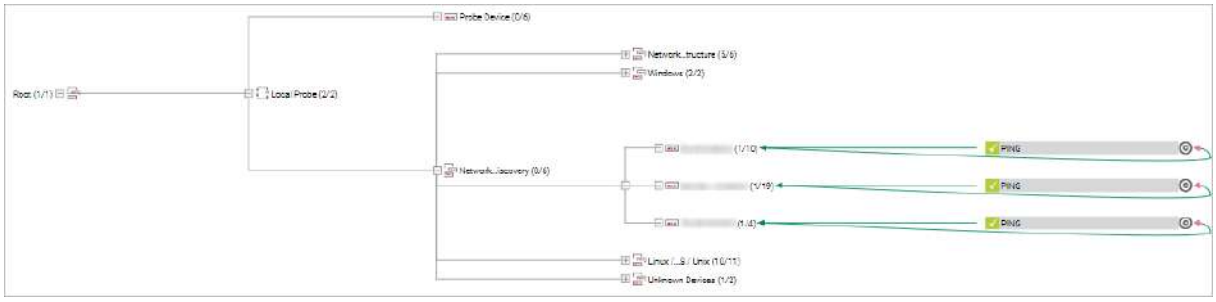
You can use dependencies to pause sensors based on the status 179 of a different (master) sensor to avoid false alarms and incorrect downtime recording. A dependency stops the monitoring of one sensor or a set of sensors as soon as the parent sensor shows the Down status or if the parent sensor shows the Paused status because of another dependency. This means, for example, that you can stop monitoring remote network services when the corresponding firewall is down because of connection problems.

When you use the auto-discovery 264 feature, PRTG sets the Ping sensor of a device as the master object for the device by default. This means that monitoring for the entire device is paused if the Ping sensor shows the Down status or if it shows the Paused status because of a dependency. Usually, it makes little sense to monitor any other parameters while the Ping sensor indicates that the device is unavailable.

ⓘ You do not trigger a status change by dependency 139 if you manually pause a master object or if you pause it by schedule 140. For more details, see the Knowledge Base: Why will dependent objects not automatically pause when I pause the master object?

ⓘ If a sensor shows the Paused status because of a dependency, the objects that use the sensor as parent also show the Paused status.

To view the list of dependencies, select Devices | Dependencies and the corresponding dependencies path from the main menu bar 248. From there you can also access the dependencies graph 3166 that visualizes all dependencies in your network.



Dependencies Graph

For more information about the dependency settings, see the settings of the object 198 for which you want to set a dependency, section Schedules, Dependencies, and Maintenance Window.

More

KNOWLEDGE BASE

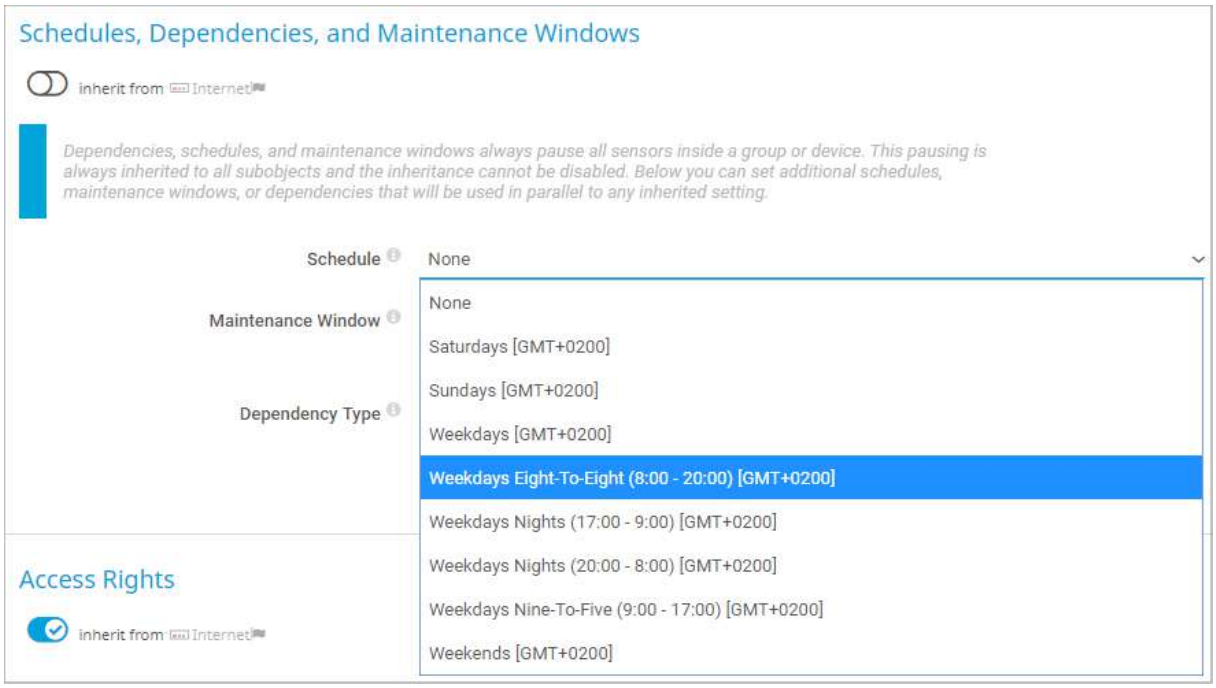
Why will dependent objects not automatically pause when I pause the master object?

- https://kb.paessler.com/en/topic/76351

5.7 Scheduling

With schedules, you can automatically pause 224 specific objects for a specific time span, for example, on Sundays between 16:00 and 20:00. A sensor in the Paused status 179 does not collect monitoring data, does not change its status, and does not trigger any notifications 141. You can also pause monitoring for planned system maintenance windows to avoid false alarms. You can apply different schedules to every object. PRTG also uses schedules for reports and notifications.

ⓘ You do not trigger a status change by dependency 139 if you manually pause a master object or if you pause it by schedule 140. For more details, see the Knowledge Base: Why will dependent objects not automatically pause when I pause the master object?



Available Default Schedules in Device Settings

Schedules are user account specific. To change the predefined schedules or to add your own schedules, see section Schedules 3284.

ⓘ If you use a cluster with cluster nodes in different time zones, the schedule applies at the local time of each cluster node. For more information, see section Failover Cluster Configuration 3631.

More

KNOWLEDGE BASE

Why will dependent objects not automatically pause when I pause the master object?

- https://kb.paessler.com/en/topic/76351

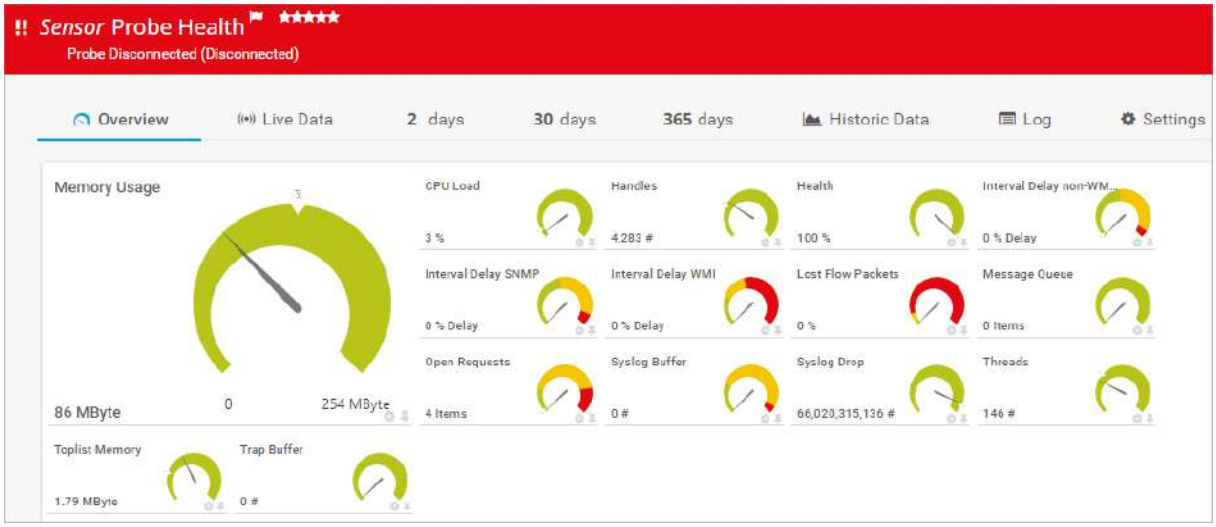
5.8 Notifying

PRTG keeps you or other responsible people informed about the status of the network. There are several methods that you can use to stay up to date.

Internal Sensor Alerts

Alerts are an important part of monitoring that informs you when there are issues, when values exceed limits, or when a sensor status changes, for example. Some sensors display internal alerts in case of errors, for example, disconnected probes or socket and timeout errors. There are also sensors whose internal sensor alerts you can modify. To see if you can modify an alert, check the sensor's settings for customizable options.

Here is an example of a sensor that is in the Down status 179 because of an internal sensor alert.



Probe Health Sensor w ith Disconnected Probe Alert

HTTP sensors, for example, show preconfigured internal alerts based on specific HTTP status codes.

For more information, see the Knowledge Base: Which HTTP status code leads to which HTTP sensor status?

Channel Limits

There are also alerts that are triggered by limits that you can set in the channel settings 3121 of a sensor. PRTG triggers a sensor status 179 change when a sensor measures values that exceed or fall below a defined limit. For example, you can set an SNMP CPU Load sensor to the Down status when it measures values that you consider critical. This sensor then appears in the alarms 199 list as well.

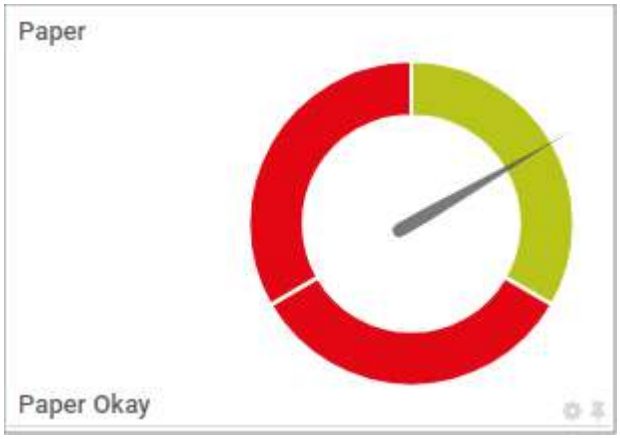
This type of alert only applies when a value breaches the configured limits. If the value is normal again in the next sensor scan, the sensor shows the Up status again.

The value type that you need to configure for limits depends on the type of data that the channel returns. You can set absolute values or delta values 3129.

For more information, see the video tutorial: How to set channel limits.

Lookups for Channels

PRTG also uses lookups for some sensors. In general, lookups make data more human friendly because they map status values that a device returns, usually integers, to more informative expressions in words that show you the status of a target device in plain text.



SNMP HP LaserJet Hardware Gauge

Additionally, lookups can define the sensor status in combination with specific status codes. For example, a sensor can show the Unknown status if a channel value, provided by lookups, indicates that the device is Inactive, instead of displaying a numeric value like -1.

You can also modify preconfigured lookups or create your own custom lookups.

For more information, see section Define Lookups 3604.

Notifications

PRTG can send a notification 3173 when it discovers, for example, downtime, an overloaded system, threshold breaches, or similar situations. Notifications use various methods 3252 to notify you of issues. After you create notification templates 3245 in the system settings, you can select the templates on the Notification Triggers tab of probes, groups, devices, and sensors, as well as the root group.

The status or the data of a sensor can also trigger notifications. With this mechanism, you can configure custom external alerts. Which notification triggers 3133 are available depends on the kind of object you edit. You can define notification triggers that are activated by an 'on change' event. Some sensors offer the option to trigger a notification whenever sensor values change.

For more information, see section Notifications 3173.

Alarms

The alarms list shows all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. Sensors in the Up, Paused, or Unknown states do not appear here.

For more information, see section Alarms 199.

Logs

The logs list shows the log file that includes all monitoring events. PRTG documents the activity of every single object, so you can use this data to check if your setup works as expected.

For more information, see section Logs 208.

Tickets

The tickets list shows tickets with important system information or actions that you need to take. We recommend that you view every ticket and take appropriate action. By default, PRTG sends an email to the PRTG System Administrator user for every new ticket that the system or a user creates. If a ticket is assigned to a specific user, this user also receives an email by default.

For more information, see section Tickets 211.

More

KNOWLEDGE BASE

Which HTTP status code leads to which HTTP sensor status?

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

VIDEO TUTORIAL

How to set channel limits

- https://www.paessler.com/support/videos-and-webinars/videos/how-to-set-channel-limits

5.9 Access Rights Management

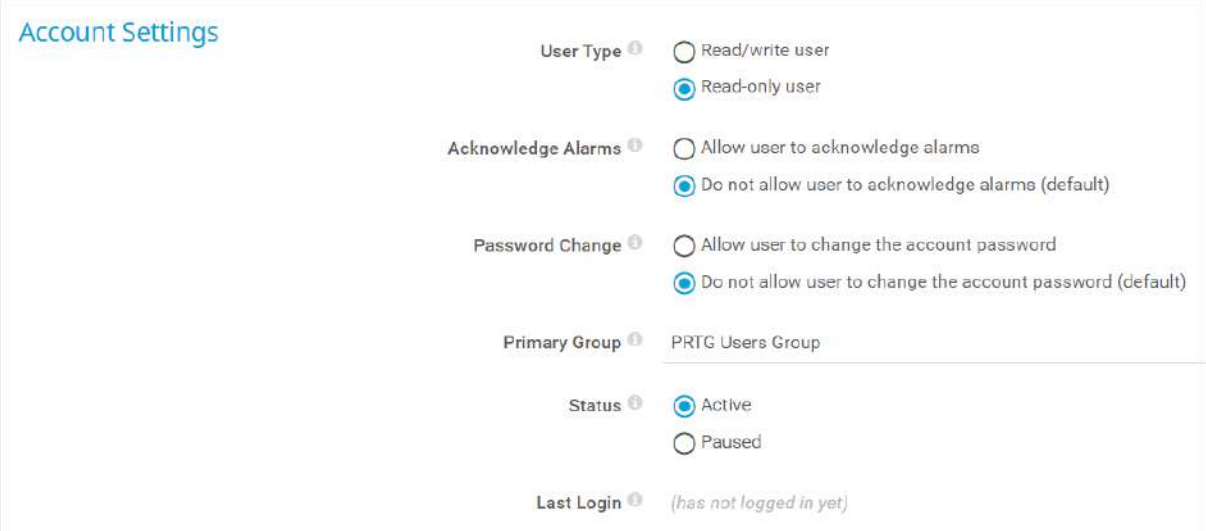
With the access rights management, you can define which user in which user group can access which objects in your PRTG installation, and you can manage all user access rights and group access rights.

You can create a nearly unlimited number of other users, which you can organize in a nearly unlimited number of user groups. Each user group can have separate access rights 144 for each object in the device tree except channels, as well as for libraries, maps, and reports. Objects can also inherit 135 access rights according to the object hierarchy 131.

User Access Rights Overview

Each user also has specific access rights. There are administrators who are user group members with administrative rights, read/write users, and read-only users. You can define the user type (read-only user or read/write user) in the user account settings.

For more information, see section User Accounts 3335.



User Access Rights in User Accounts Settings

Individual user access rights, combined with the access rights of the groups that the user is a member of, determine the access rights for device tree objects, libraries, maps, and reports. In general, group access rights override user access rights unless a user is a read-only user. Read-only users always have only read access.

You can define the group access rights for each object in the device tree via the corresponding context menus 226 or in the object settings 198.

Group Access Rights Overview

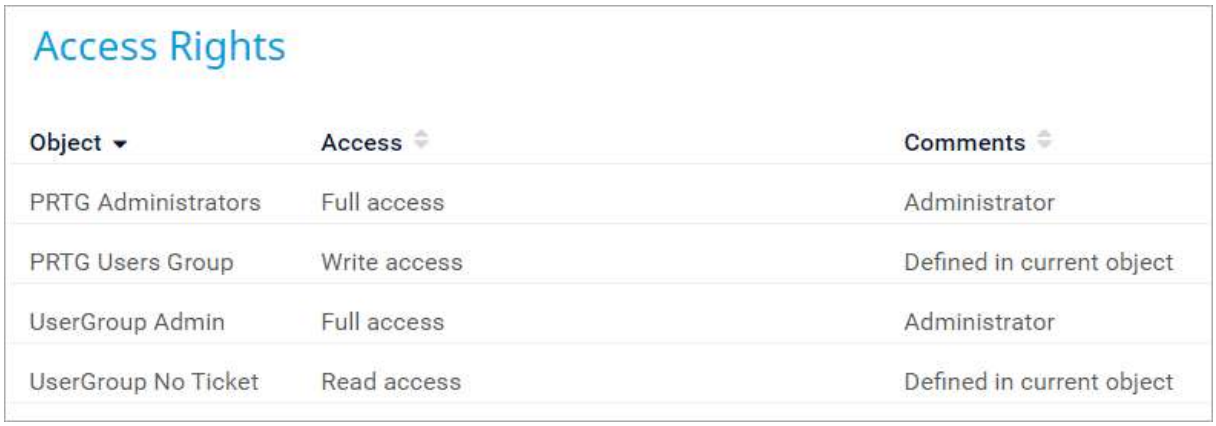
The following classes of group access rights are available, in hierarchical order (from the lowest group access right to the highest group access right).

The access rights apply to device tree objects and to libraries, maps, and reports.

Group Access Rights	Description
No access	The members of the user group cannot see or access the object. They also cannot see or access logs, tickets, or alarms for the object.
Read access	The members of the user group can only view the object and its settings. ⓘ Read-only users who have been explicitly allowed to acknowledge alarms and read/write users in a user group that has read access can still acknowledge alarms. For more information, see section User Accounts 3339.
Write access	The members of the user group can view the object and edit its settings. They can also add and delete objects, acknowledge alarms, edit notification templates, notification contacts, and schedules.
Full access	The members of the user group can view the object and edit its settings. They can also add and delete objects, acknowledge alarms, edit notification templates, notification contacts, and schedules. In addition, they can edit group access rights for objects.

If a user group has administrative rights, all user group members always have full access to every object in the device tree, library, map, and report, and all other functionalities and features of PRTG.

ⓘ Group access rights that you define directly on an object, for example a device, override inherited rights. If you do not define group access rights directly on an object, PRTG checks the next object that is higher up in the object hierarchy for group access rights until there is no higher-level object available.



Different Access Rights Depending on User Groups

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

Group Access Rights in Combination with User Access Rights

The following table shows the correlation between group access rights and user access rights. The table applies to both PRTG user groups and Active Directory groups, as well as to both PRTG users and Active Directory users. The column headings show the group access rights to an object. The row headings show the type of user.

Group Access Rights and User Access Rights Combined				
	User group has read access to an object	User group has write access to an object	User group has full access to an object	Administrator group
Read-only user	Read access	Read access	Read access	n/a
Read/write user	Read access	Write access	Full access	Full access
Administrator	Full access	Full access	Full access	Full access

The following rules apply:

- Read-only users
  - always have only read access, no matter what access rights you define for the user groups they are members of
  - can never see or use the ticket system
  - can acknowledge alarms and change their own password in their user account settings, if an administrator allows them to
  - can never be members of user groups with administrative rights
- Read/write users
  - can use the ticket system if the user group they are members of has access to the ticket system
  - can acknowledge alarms
  - can change their own password
  - can have full access to device tree objects, libraries, maps, and reports, if the user group they are members of has full access to the respective object
  - always have administrative rights if they are members of a group with administrative rights
- Administrators
  - are members of groups with administrative rights
  - have no access restrictions at all

- can also manage user accounts, user groups, and cluster setups
- can change the monitoring configuration of PRTG

ⓘ If a user is a member of more than one user group, the group access rights of the user group with the highest access rights apply.

5.10 Data Reporting

With PRTG, you can view, analyze, and review monitoring data for specific time spans. There are several ways to create customized data reporting.

View Historic Sensor Data

To get an overview of a single sensor's historic data, you can generate historic data reports via the sensor's Historic Data tab.

- For more information, see section Historic Data Reports 183.

Generate Reports

In addition to reports about a single sensor's historic data, you can also create comprehensive and detailed reports for all monitoring data.

- For more information, see section Reports 3192.

Export Data with the PRTG API

You can also export all raw monitoring data to .xml or .csv files and generate your own reports with any third-party software.

- For more information, see section Application Programming Interface (API) Definition 3511.

Make Data Available

You can make monitoring data available to others via a specific read-only user, or you can create public HTML pages to display your monitoring data via the Maps feature.

- For more information, see section Access Rights Management 144 and section Maps 3214.

5.11 IPv6 Support

PRTG supports the IPv6 protocol for most sensors. You can choose whether you want to query data from your network devices via an IPv4 or IPv6 connection. Specify your preference in the device settings 588. The sensors you add to the device use the protocol that you select.

In the IPv6: Outgoing IP for Monitoring Requests setting of the PRTG Administration Tool 3486, you can additionally select the IPv6 address that PRTG uses for outgoing monitoring requests. The same option is also available for IPv4.

Not all sensors are IPv6 compatible. Incompatible sensors are not selectable on IPv6 devices. For an overview list of all sensors, including the IP version that they support, see section List of Available Sensor Types 3683.

The hosted probe of a PRTG Hosted Monitor instance does not support the IPv6 protocol. If you want to use sensors that support IPv6, add them to a remote probe device.

Part 6
Basic Procedures

6 Basic Procedures

The following sections introduce the basic features and concepts of PRTG.

- Login 152
- Welcome Page 156
  - Customer Service 161
- General Layout 164
- Sensor States 179
- Historic Data Reports 183
- Similar Sensors 189
- Recommended Sensors 194
- Object Settings 198
- Alarms 199
- System Information 202
- Logs 208
- Tickets 211
- Working with Table Lists 216
- Object Selector 219
- Priority and Favorites 221
- Pause 224
- Context Menus 226
- Hover Popup 245
- Main Menu Structure 247

6.1 Login

For PRTG Network Monitor, you can log in to the PRTG web interface once the PRTG core server is installed. In your browser, open the IP address or Domain Name System (DNS) name of the PRTG core server system and click Log in.

You can look up and change the web server settings of PRTG Network Monitor at any time in the PRTG Administration Tool 3469 on the PRTG core server system. In particular, when you access PRTG from the internet, you should use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. To secure your connection, click Switch to SSL/TLS under Enable SSL/TLS for the PRTG web interface on the welcome screen.

Load the PRTG Web Interface

In a web browser, enter the IP address or URL of the PRTG core server system. If you use a cluster, connect to the master node. You can also double-click the PRTG Network Monitor desktop icon on the PRTG core server system.

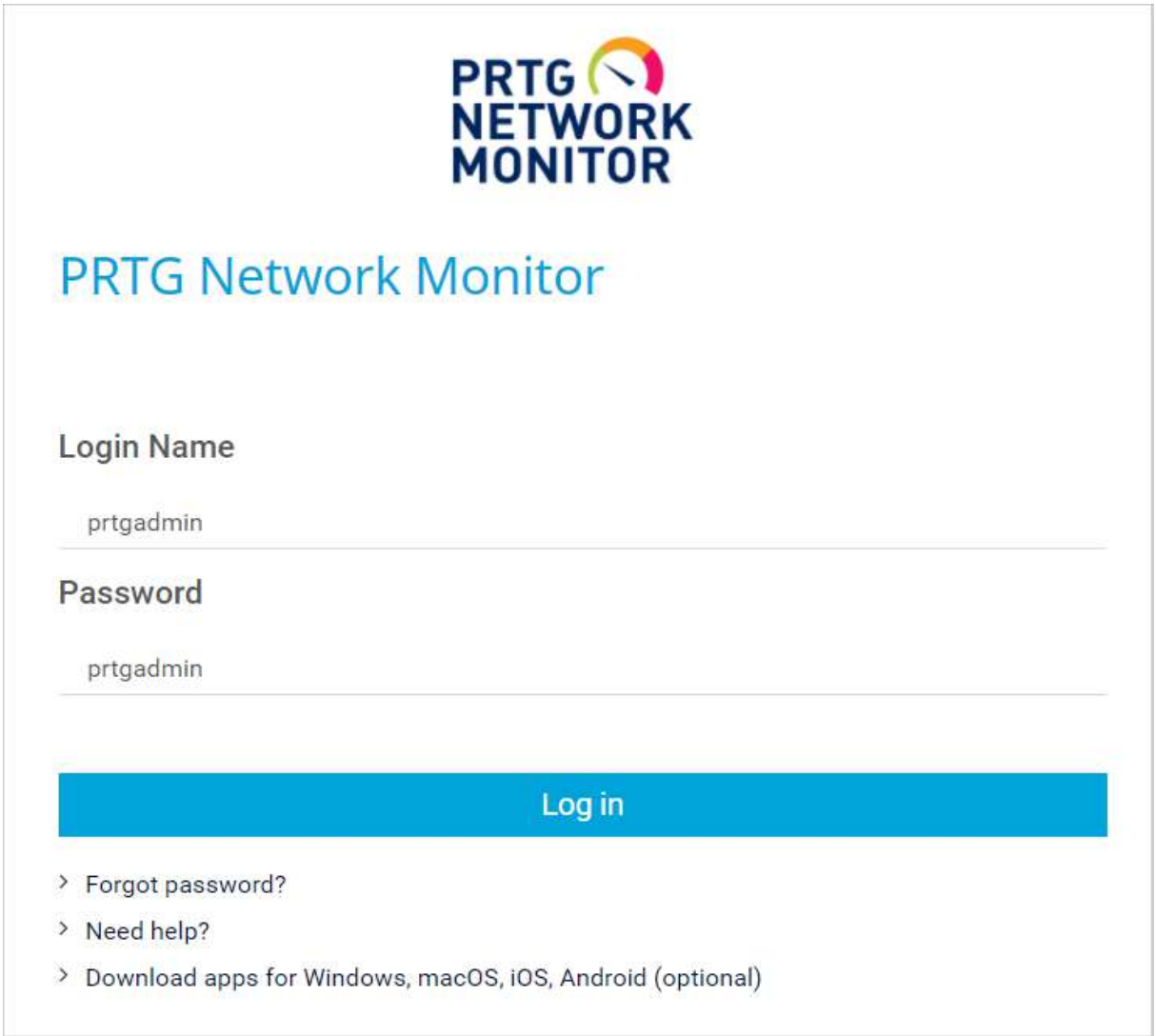
If you run PRTG on localhost, do not use the DNS name http://localhost to log in to the PRTG web server, as this might considerably slow down the PRTG web interface. Use your local IP address or http://127.0.0.1 instead.

If you see an SSL certificate warning in your browser, you can usually confirm it.

For more information, see Knowledge Base: Why does my browser show an SSL certificate warning when I open the PRTG web interface?

Login Screen

After loading the PRTG web interface, the login screen is visible. You can either log in as the predefined PRTG System Administrator user or as any other user. As an administrator, you can use all functionalities of the PRTG web interface. Administrators can create additional users 3335 with administrative rights or users with more restricted user access rights (for example, read-only users).



Login Screen

Log In as Predefined Administrator (First Time Login)

This only applies to PRTG Network Monitor, not to PRTG Hosted Monitor.

When you log in for the first time, the login name and password for the predefined PRTG System Administrator user account are both prtgadmin. PRTG automatically fills in the default credentials and shows the password in plain text.

After login, you should change the default password. To do so, go to Setup | Account Settings | My Account and specify a new password in section User Account Settings.

If you are not logged in to the PRTG web interface, you can change the credentials for the predefined user account at any time in the PRTG Administration Tool.

If you enter a different login name or change your password, the password is no longer shown in plain text.

Log In as User

If you received user credentials from your system administrator, enter them in the login screen to log in to the PRTG web interface. This also applies if you use other administrator credentials.

Login Options

- Log in: Log in to the fully featured PRTG web interface. We recommend that you use this option for PRTG whenever possible. It offers the full functionality of PRTG. Use Google Chrome 72 or Mozilla Firefox 65 for best performance.
  - Although you can log in with Microsoft Internet Explorer 11, the PRTG web interface might not be fully compatible with Internet Explorer. If you use Microsoft Internet Explorer 11, set the security level to Medium-high (or lower) and make sure that no Compatibility View is enabled.
- Download apps for Windows, macOS, iOS, Android (optional): Opens Setup | Optional Downloads in the PRTG web interface. You can optionally download 3406 the PRTG apps 3420 for iOS or Android or PRTG Desktop 3417.
  - If you use this download option, you require your login name and password (or the default credentials) for the login.

Only Google Chrome 72 and Mozilla Firefox 65 are fully compatible with the PRTG web interface.

Enter specific credentials or use the default credentials that PRTG fills in automatically. Click Log in to proceed to the PRTG web interface.

Recover Password

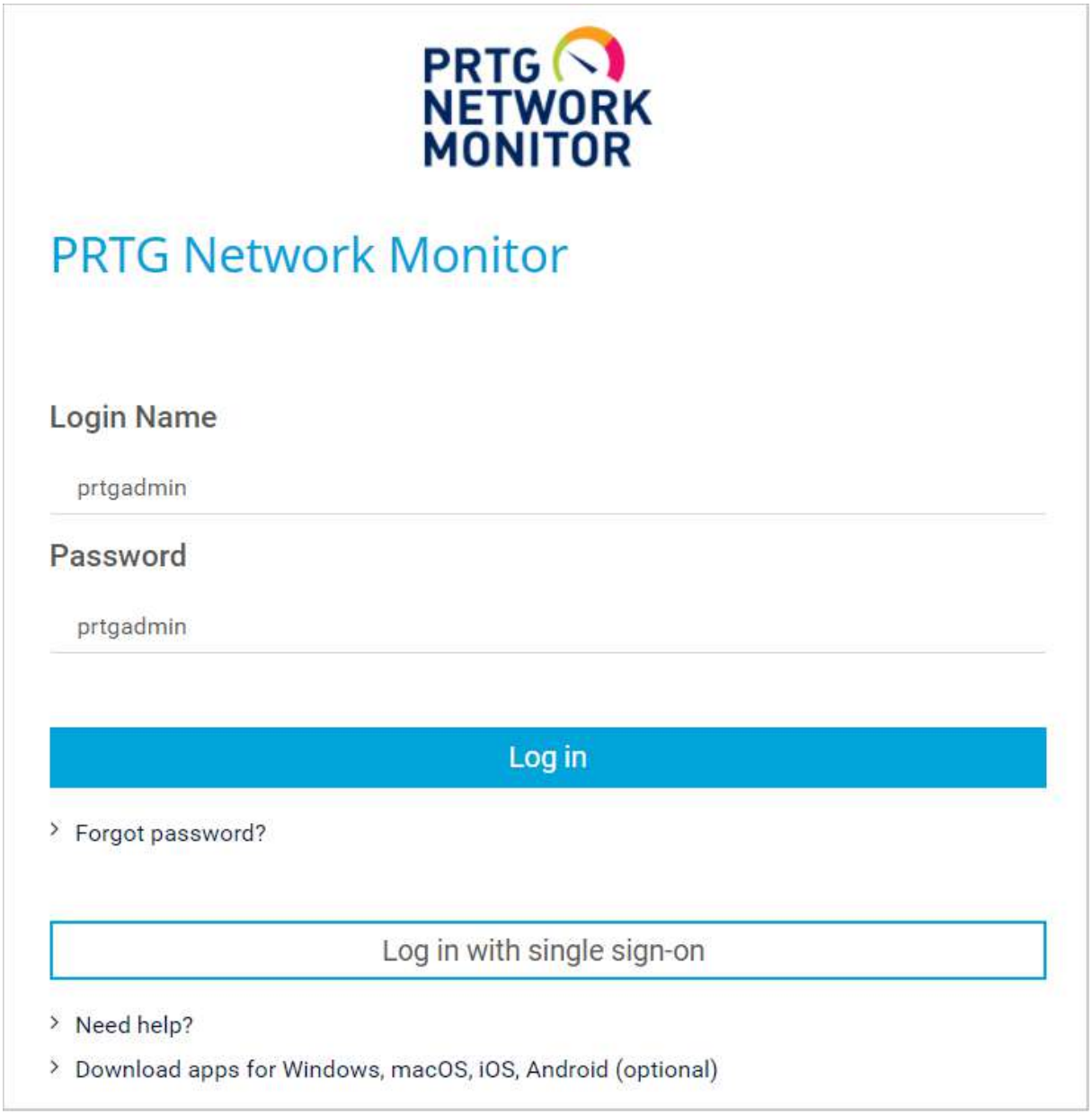
If you cannot remember your PRTG Network Monitor password, click the Forgot password? link. The Password Recovery page opens. Enter your Login Name, click Request a New Password, and PRTG sends an email to the primary email address of your user account. Click the link in the email to set a new password. The link is valid for 60 minutes. Enter a New Password, then enter it again under Confirm Password. Click Set New Password to change your password.

The password must be at least 8 characters long and must contain a capital letter and a number.

When the password is successfully reset, all active user sessions of this user account are logged out. Log in again with the new password.

Login Screen with Single Sign-On (SSO)

After you configure SSO 3358, you see a new button on the login screen of the PRTG web interface.



Log in with SSO

Click Log in with single sign-on to continue with the login procedure of the single sign-on provider. After finishing the login procedure, you will be transferred back to PRTG.

More

KNOWLEDGE BASE

Why does my browser show an SSL certificate warning when I open the PRTG web interface?

- https://kb.paessler.com/en/topic/89984

6.2 Welcome Page

After you completed the smart setup 42, you see the Welcome page by default when you log in to the PRTG web interface. The collected information about your PRTG installation makes the page a good starting point for your daily monitoring activities. You can set a different home page in your account settings 3243. Of course, you can also use the Maps 3214 feature to create customized dashboards that you can use as your home page.

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

Welcome to PRTG

Sensor Overview

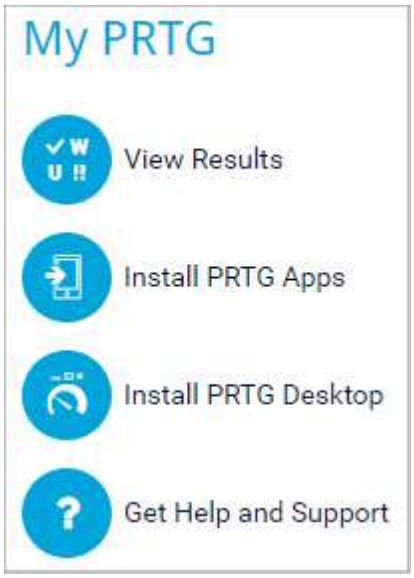
The Welcome page displays various information about your PRTG installation and is similar to a dashboard. It keeps you informed about all sensors and alarms:

Sensor Overview on the Welcome Page

- Click Sensors to open the top 10 lists 251 for sensors.
- Click View All Alarms to open a list of alarms 199 in your installation.
- Click a sensor status 179 to open a list of all sensors with the corresponding status.

My PRTG Section

In the My PRTG section, you can directly access different pages in the PRTG web interface.



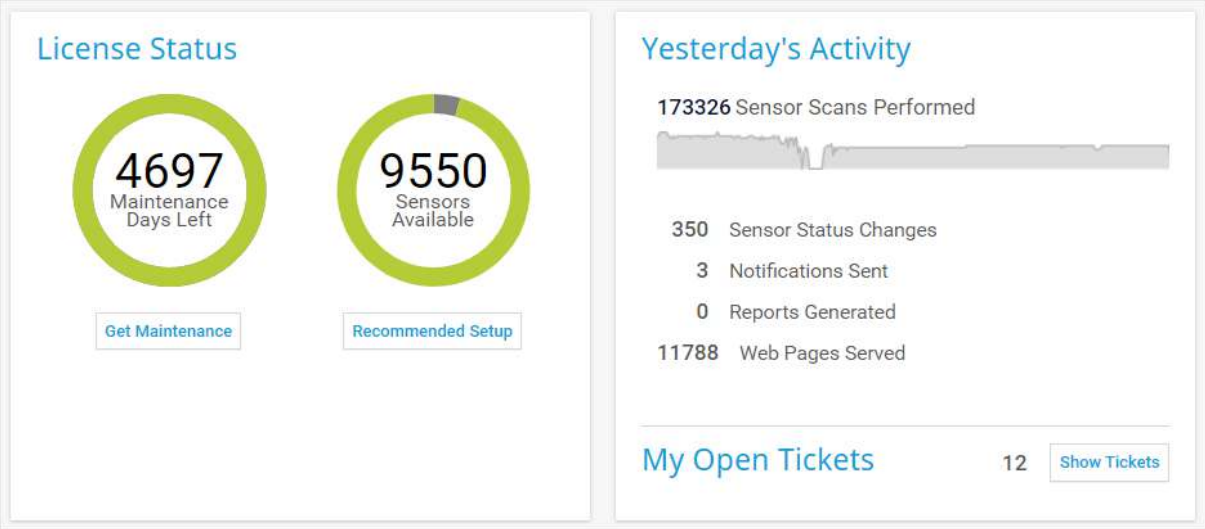
My PRTG Section on the Welcome Page

Option	Description
View Results	Open the device tree 164 that shows your monitoring results.
Install PRTG Apps	Open the download page for the PRTG apps for iOS or Android 3406.
Install PRTG Desktop	Open the download page for PRTG Desktop 3406.

Option	Description
Get Help and Support	Open the Help and Support Center 3408 from where you can access the PRTG Manual, the Knowledge Base, and video tutorials. You can also open support tickets 3409 and contact our customer service 161 from this page.
Manage Subscription	This option is only visible if you use PRTG Hosted Monitor. Open your PRTG Hosted Monitor dashboard and manage your subscriptions.

Other Sections

Other sections are, for example, the License Status section, the Yesterday's Activity section, the Paessler Blog section, and the Update Available section.



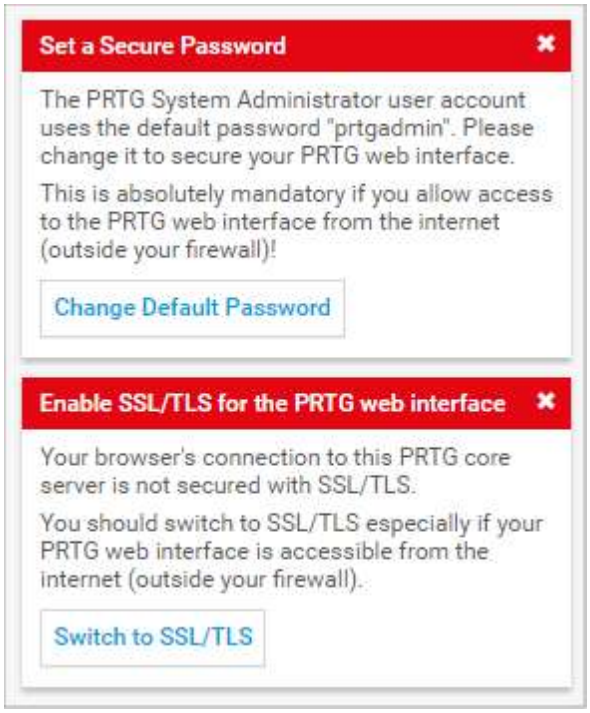
License Status Section and Yesterday's Activity Section on the Welcome Page

Section	Description
License Status	Shows the number of your remaining maintenance days for PRTG Network Monitor and the number of sensors that you can still add with your license. Click Get Maintenance to open the Paessler shop and extend your maintenance for PRTG Network Monitor installations. Click Get More Sensors to open the Paessler shop and upgrade your license. See also section License Information 3395. ⓘ For technical reasons, the number of available sensors that is displayed here does not include sensors in the Paused status because they do not count towards the maximum number of sensors that your license allows. Add the number of your sensors that are in the Paused status to the displayed number to know exactly how many sensors are still available on your installation.

Section	Description
	ⓘ If you use a PRTG Network Monitor license with an unlimited number of sensors, PRTG takes 10,000 sensors as the starting point to calculate the number of available sensors that is displayed here. Consider the system requirements 23 for a recommended PRTG core server setup and click Recommended Setup for more information.
Yesterday's Activity	Shows what your PRTG core server or PRTG Hosted Monitor instance did for you on the day before. Hover over the mini graph to show the number of sensor scans on a specific day. See also the Activity History in section System Status 3381. Click Show Tickets under My Open Tickets to display all open tickets that are assigned to you.
Paessler Blog	Shows recent information about PRTG and Paessler. Click the heading of an article to open it on the Paessler website.
Update Available	This section is only visible if an update is available. It shows the version number of your PRTG Network Monitor installation and the version number of the latest available PRTG version. You see the label NEW if a newer version is available. Click Install Update to open the Auto-Update 3402 page.

Further options

There are some further options on the Welcome page, for example, you can set a secure password or enable SSL/TLS for the PRTG web interface.



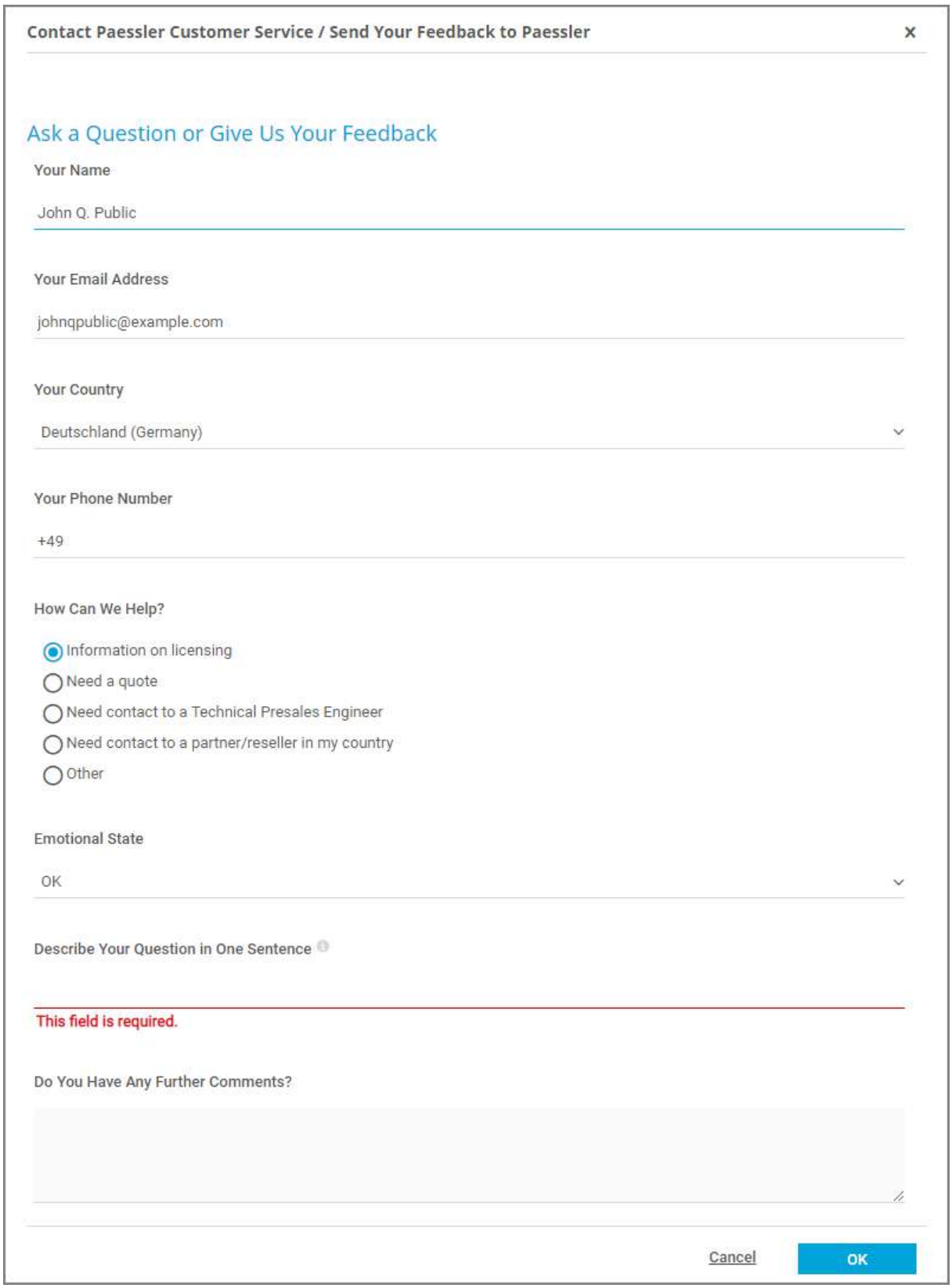
Further Options on the Welcome Page

- If your PRTG Network Monitor installation is not Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured, PRTG asks you to enable SSL/TLS for the PRTG web interface. Click Switch to SSL/TLS and in the Do you want to switch to SSL/TLS? dialog, click Yes, switch to SSL/TLS to enable SSL/TLS. See also section User Interface 3293. Click ✖ to remove this note.
- If you still use the default password of the PRTG System Administrator user (prtgadmin) for PRTG Network Monitor, PRTG asks you to set a secure password if your PRTG web interface is publicly available. Click Change Default Password to define a new password. See also section User Accounts 3337. Click ✖ to remove this note.
- In the video section, you find informative videos about monitoring with PRTG. Click a video to open it and play it on the Paessler website.

6.2.1 Customer Service

If you have any questions about license purchases, upgrades, or maintenance extensions, you can directly contact the Paessler Customer Service from the Help and Support Center 3408 in the PRTG web interface. We readily assist you with quotes or information about licenses and maintenance, and guide you through the purchasing process. Our Customer Service team is also happy to send you the contact information of a knowledgeable PRTG partner in your region or research any technical specifications you might need beforehand.

ⓘ PRTG securely transmits your feedback or questions to Paessler via the PRTG Cloud. Make sure that your PRTG core server has access to the internet and can reach the URL https://api.prtgcloud.com:443 for successful transmission.



Contact Paessler Customer Service Form

Ask a Question or Give Us Your Feedback

Provide the following information in this section of the Contact Paessler Customer Service form.

Field	Description
Your Name	Enter your full name for contact information.
Your Email Address	Enter an email address with which we can reach you.
Your Country	Select the country in which you run PRTG so that we can provide you with contact information for a partner nearby.
Your Phone Number	Enter a phone number with which we can reach you.
How Can We Help?	Select the scope of your question.
Emotional State	If you want to, you can indicate your feelings about PRTG and your purchase process.
Describe Your Question in One Sentence	Provide a short description that indicates the topic of your request.
Do You Have Any Further Comments?	Enter your comments here. This can be feedback or any questions for our customer service.

Click OK to send your question or feedback to our customer service. Click Cancel to close the customer service contact form without sending it.

If you have technical questions about your setup, contact the Paessler support team 3409.

6.3 General Layout

This section provides a general overview of the structure of the PRTG web interface. The central focus is the Devices view, which you can select via the main menu bar 248. The Devices view presents the device tree and your monitoring results.

In this section:

- Welcome Page 164
- Device Tree View Layout 164
- Navigation 167
- Global Header Area 168
- Page Header Bar 170
- Page Content 171
- Switch Device Tree View 173
- Classic Device Tree View 174
- Extended Device Tree Views 174
- Add Button 177
- Default Objects in the Device Tree 177
- Priority and Favorites 178

Welcome Page

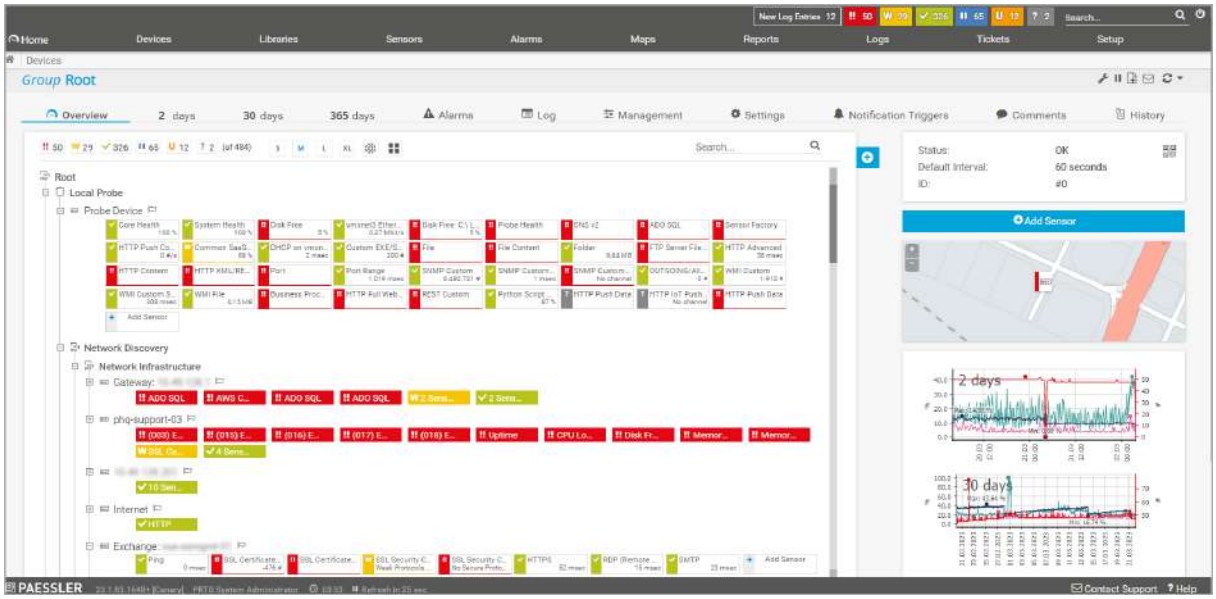
When you log in to the PRTG web interface, you see the Welcome page 156 by default. You can set a different home page in your account settings 3243.

Click View Results to open the device tree.

Device Tree View Layout

Click View Results on the Welcome page or select Devices from the main menu bar to display the device tree.

Device Tree



Device Tree

From top to bottom, the device tree page has several areas that are covered in further detail in this section. For a general overview of the device tree page, see the table below.

Global Header Area

Global Header Area

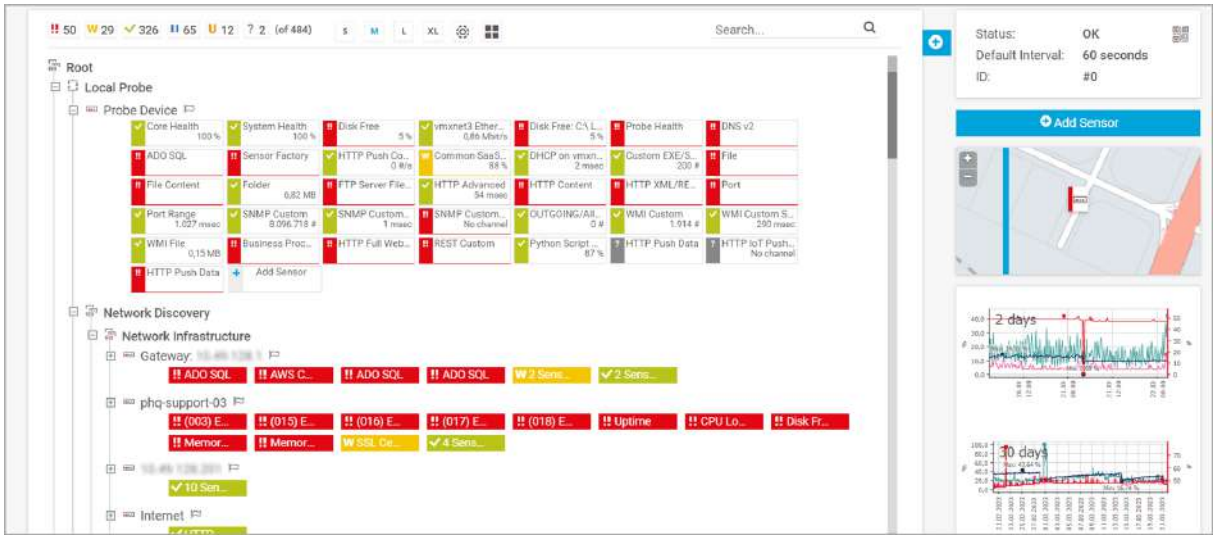
Item	Description
Global header area 168	This area contains the main menu bar at the very top, the global status bar, breadcrumbs that show the path to the selected object, a quick search box, and the logout button.

Page Header Bar

Page Header Bar

Item	Description
Page header bar 170	This area contains the page heading with the name of the selected object, several tabs with settings, and quick action buttons.

Page Content



Page Content

Item	Description
Page content 171	This area contains information about the selected object and all other objects underneath in the device tree hierarchy, the object's status bar, a quick search box, the QR code that links to the URL of the selected page, and graphs for different time spans.

View Options

View Options

Item	Description
Viewing options 173	These buttons are part of the page content. Here you can adjust how your device tree is displayed.

Footer Section

Footer Section

Item	Description
Page footer	This area shows information about the version of PRTG, the logged in user account, and the time (depending on the time zone settings 3342 for the logged in user). A timer counts down how much time remains until the next automatic page refresh. Click to pause the refresh timer and click to resume. If you open a different page while the refresh timer is paused, the timer resumes automatically and starts with the defined Refresh Interval (Sec.) that you can configure in your account settings. Long table lists 216 that are set to display 1000 items at a time are excluded from the automatic refresh to ensure system performance.
Page footer icons	Click for quick access to the auto-update 3402 settings if a new version is available. To open the Contact Support form 3409, click . For context-sensitive help, click . If you run PRTG in a cluster, you also see a cluster-related element. It shows the name of the cluster node that you are logged in to and displays whether this is a master node or a failover node. Click the bar to show the cluster status 3393. On a failover node, you can review all data, but PRTG does not save changes in the settings. To change the settings, log in to the master node.

Navigation

To navigate the PRTG web interface, the following options are available:

- The main menu bar provides access to all important aspects of the software.
- The quick search is often the fastest way to find a specific object (for example, a sensor or a device).
- The clickable breadcrumbs show the path to a selected object in the object hierarchy.
- Click an object to see its details. In the page heading of the page header bar, you always see the name of the object that you have selected.
- Use the page tabs to switch between various subpages.
- Right-click objects to open their context menu 226.
- Hover over objects to display tool tips. Hover longer to open a quick-access window (hover popup 245).
- Drill down into the object hierarchy of probes, groups, devices, and sensors in the device tree. To do so, click a subobject of the displayed object (for example, click a sensor on the Overview tab of a device).

These navigation options offer complete access to the functionality of PRTG.

In the following sections, we describe the different areas of the PRTG web interface.

Global Header Area

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.

Global Header Area

Global Header Area

The global header area of the PRTG web interface provides important, very condensed information about your installation and offers access to all content and settings. The following table lists the elements that make up the global header area.

Main Menu Bar

Main Menu Bar

Item	Description
Main menu bar	To navigate the PRTG web interface, the main menu bar is the best starting point. We recommend that you take a few minutes to familiarize yourself with the main menu bar and its submenus. For more information, see section Main Menu Structure 247.

New Alarms

New Alarms

Item	Description
New alarms, New log entries, Updated tickets	The information boxes show how many new alarms, new log entries, and updated tickets have occurred. Click the respective box to view the lists of alarms 199, logs 208, or tickets 211.

Global Sensor Status Symbols

Global Sensor Status Symbols

Item	Description
Global sensor status symbols	This area shows the accumulated states of all configured sensors, grouped into the different sensor states. You see boxes with numbers that show the amount of sensors that are in the respective status. For example, you can see how many sensors are in the Up, Down, or Warning status. Click a box to view a list of all sensors that are in the respective status. For more information, see section Sensor States 179.

Search Box

Search Box

Item	Description
Search box, log out	You can start a search ( ) or log out ( ) via the respective buttons in the top-right corner. To search for an object, enter a name, parts of a name, an IP address, a Domain Name System (DNS) name, or a tag in the search box and confirm with the Enter key. PRTG performs a string search in your entire monitoring setup, including groups, devices, sensors, libraries, maps, reports, tickets, and object comments. A page with items and online help articles that are related to the search term opens.

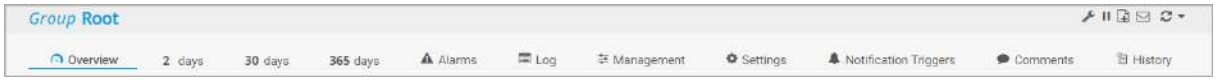
Breadcrumbs

Breadcrumbs

Item	Description
Breadcrumbs	Below the main menu bar, PRTG shows a path that retraces the steps back to the Welcome page (or your defined starting page). Use these breadcrumbs to navigate back to where you came from. If you click on a breadcrumb item, a dropdown list opens that shows all objects on the same level. You can either search for an object or select one directly. For example, you can directly access all other sensors on a device, other devices within a group, and other groups on the same probe. Other probes in your root group are also available.

Page Header Bar

ⓘ This documentation refers to an administrator that accesses the PRTG web interface on a master node. Other user accounts, interfaces, or failover nodes might not have all of the options in the way described here. In a cluster, note that failover nodes are read-only by default.



Page Header Bar

The page header bar below the global header area consists of the following elements.

Page Heading

Page Heading

Item	Description
Page heading	The page heading displays the selected object's type and name. In the screenshot, this is the group that is called Root. Here you can define the object's priority as well. To do so, click one of the five stars (★★★☆☆) next to the object's name (this setting is not available for the root group). For more information, see section Priority and Favorites 221.

Quick Action Buttons

Quick Action Buttons

Item	Description
Quick action buttons	On the right-hand side, there is a row of icons for several actions. Depending on the selected page, you can pause ( ) and resume ( ) the object. You can also open the settings of the object ( ), add a ticket ( ), send a link to the selected page per email ( ), or perform an immediate scan ( ). Click to open the context menu of the selected object for further options. For more information, see section Context Menus 226.

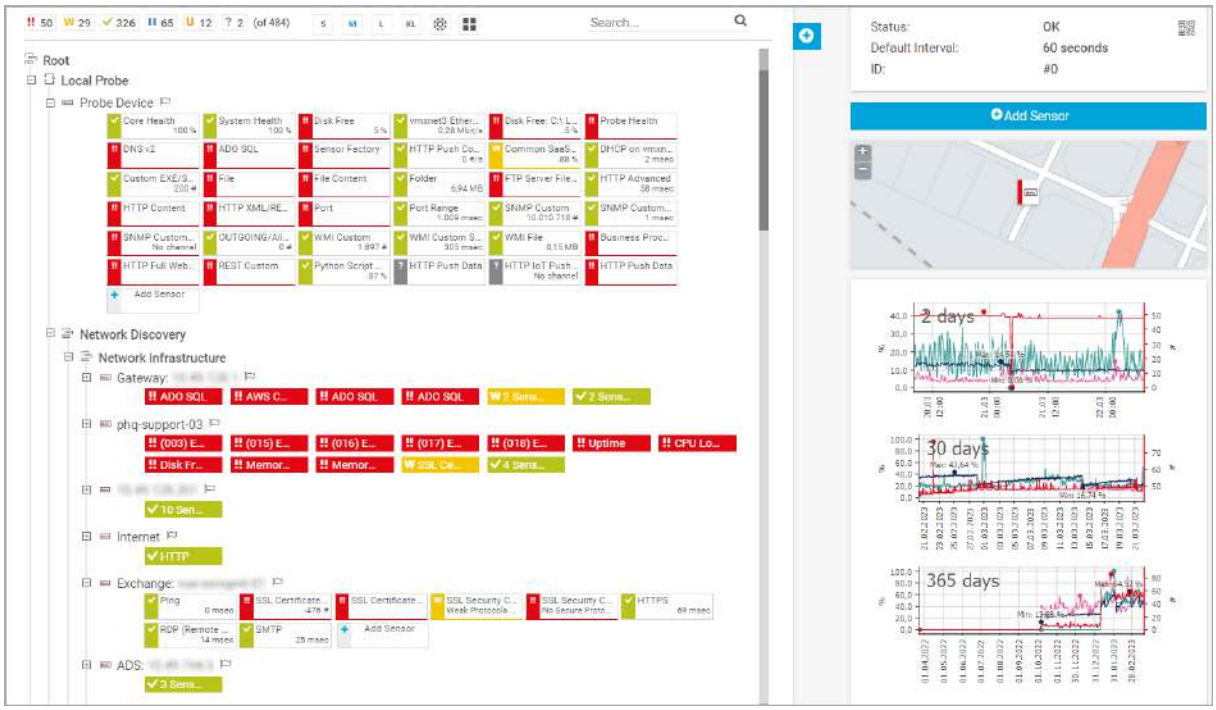
Tabs General Layout

Tabs General Layout

Item	Description
Tabs	Via tabs, you can navigate to the various subpages of an object, for example, to its monitoring data or settings. For more information, see section Object Settings 198 and the Knowledge Base: What options do I have to review my monitoring data in detail?

Page Content

The page content of the general layout varies depending on the selected object. It shows information about the object and all other objects underneath in the object hierarchy. The deeper down in the hierarchy you can find a selected object, the more detailed is the displayed information.



Page Content

Sensor Status Bar

Sensor Status Bar

Item	Description
Sensor status bar	This element is visible when you view a probe, a group (including the root group), or a device. It is not available on the Overview tab of a sensor. The sensor status bar shows the accumulated states of all sensors for the selected object, grouped into different sensor states. They show the number of sensors that are in the respective status. For example, you can see how many sensors are in the Up, Down, or Warning status. You can hide sensors that are in a certain status by clicking the respective status icon. To show the sensors again, click the status icon again. For more information on sensor states, see section Sensor States 179 .

View Options

View Options

Item	Description
Viewing options	This element is only visible when you view a probe or a group. It is not available when you view device or sensor details. For a detailed description, see Switch Device Tree View 173 below.

Device Tree Search

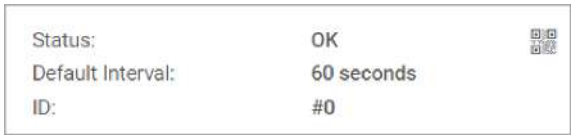
Device Tree Search

Item	Description
Device tree search	In the search box to the right of the viewing options, enter a keyword to search the device tree for matching items. The device tree highlights matching devices and sensors by graying out all others. This gives you a quick overview of sensors that monitor a specific part of your network. For example, you can enter the keyword firewall to highlight devices and sensors that match this string.

Add Button

Item	Description
Add Button	Click to add new objects to your monitoring setup. For a detailed description, see Add Button 177 below.

Object Status



Object Status

Item	Description
Object status, Scanning interval, Object ID, QR code	This element displays the status of the selected object, the interval in which PRTG scans the object, the ID of the object, and the QR code for the selected page. If you use a PRTG app for iOS or Android 3420, you can scan the code to directly view the object on your mobile device. Click the QR code to enlarge it for scanning. Depending on the object type, this element shows additional information: ▪ All objects underneath the root group show their dependency 139. ▪ Groups and devices display the time that has elapsed since the last execution of the auto-discovery 264 on the selected object. ▪ Devices show their DNS name or IP address as defined in the device settings 588 and the time that has elapsed since the last execution of the sensor recommendation 194 on this device. ▪ Sensors show additional monitoring statistics as well as their performance impact 3385.

Switch Device Tree View

Wherever a probe or group is displayed, you can choose between a number of viewing options.

Device Tree Viewing Options

Device Tree View ing Options

Classic Device Tree View

Collapsed Device with Summarized Up and Unusual States and Individual Down States

Via the Switch Device Tree View buttons in the page header bar, you can adjust how much information is included next to each object. Use the buttons to switch from a very condensed view (S) to a very spacious view (L). Use XL to switch the device tree to a list view.

In the classic device tree view, you can collapse devices, groups, and probes. Click ⊟ left of the object name to summarize the sensors according to their respective status. By default, sensors in the Down, Down (Partial), or Down (Acknowledged) status are summarized if there are more than ten sensors with the same status, otherwise they are displayed individually.

Extended Device Tree Views

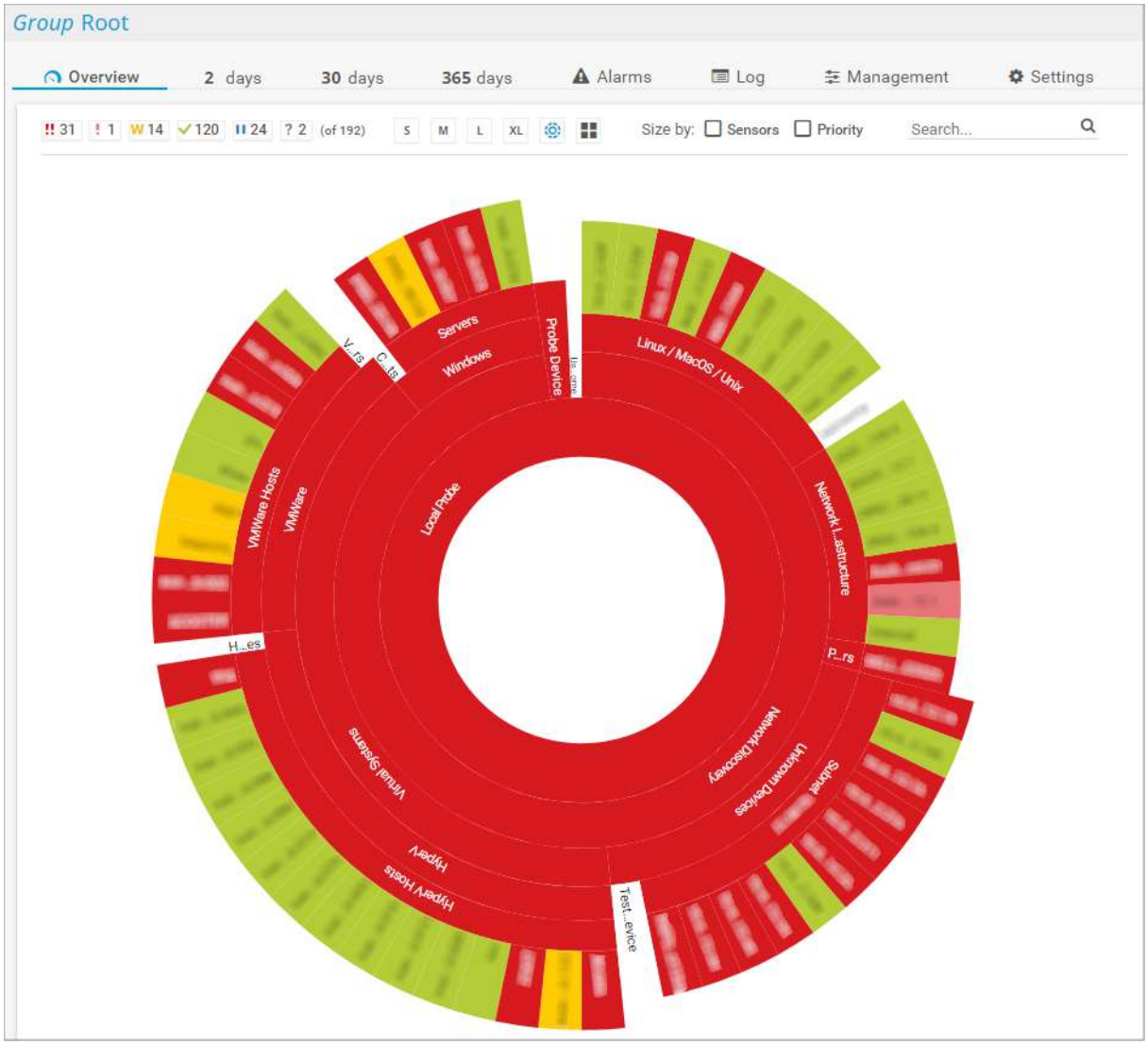
There are two additional options to the classic device tree view with which you can display the status of all sensors of your entire installation in a single overview. Click to change to the sunburst view. To change to the tree map view, click .

Sunburst View

The sunburst view displays your entire installation as a circle diagram. The groups are represented as inner circles, and all devices that belong to a group are shown as 'cake slices' that are attached to the outside of a circle element.

The sunburst is interactive:

- You can click elements to open the Overview tab of your monitoring objects.
- You can zoom in and out with your mouse wheel while pressing the Ctrl key.



Sunburst View

Tree Map View

The tree map view displays all devices of your entire installation as tiles that are sorted into a square and that are arranged according to the groups they belong to. Each device dynamically changes color to reflect the overall status of the sensors on the device.

Tree Map View

The following aspects apply to both the sunburst view and the tree map view:

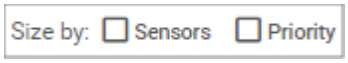
Colors

A device or group can have different colors, depending on the states of the sensors that are on the device or in the group. The sensor states are ranked according to their priority, for example, the Down status has a higher priority than the Warning status, which has a higher priority than the Up status.

For an overview of the colors and their states, see section Sensor States 179.

Size by: Sensors / Size by: Priority

You can adjust the size of the different squares according to the number of sensors that run on a device or in a group, or the sensors' priority 221, or both. Select the check boxes in the page header bar to change the square size.

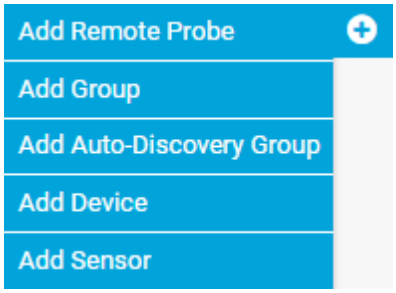


Check Boxes for Adjusting the Square Size

Add Button

Hover over to add new objects to your monitoring setup. An assistant appears and guides you through the necessary steps.

ⓘ The content of the menu varies depending on the selected object.



Add Button Menu

See the following sections for more information:

- Add Remote Probe 3619
- Add an Auto-Discovery Group 268
- Add a Group 320
- Add a Device 364
- Add a Sensor 413

Default Objects in the Device Tree

By default, PRTG Network Monitor creates a probe device on the local probe or on the hosted probe (PRTG Hosted Monitor). The probe device represents the probe system. PRTG automatically monitors the system health of the PRTG core server and each probe to discover overload that might distort monitoring results. To monitor the status of the probe system, PRTG automatically creates the following sensors:

- Core Health
- Probe Health
- System Health
- Some device-specific sensors for disk usage and bandwidth.

In a cluster, PRTG also creates a cluster probe device with a Cluster Health sensor that monitors the system health of the cluster.

Priority and Favorites

You can mark a device or sensor as a favorite. To do so, click to the right of the respective object in the device tree. The flag turns dark gray. To remove an object from your favorites, click . The flag turns transparent again.

One-Click Favorites in the Device Tree

The favorite flag for sensors is available for the L or XL viewing options.

A quick way to set the priority of an object is via the five stars in the page header bar 170 next to the object name. Click the stars to adjust the priority. ★★★★★ means top priority, ★☆☆☆☆ means lowest priority.

One-Click Favorite and Priority in the Page Header Bar

You can also add any device or sensor to your favorites in the page header bar of the respective object. To do so, click for a device or for a sensor. Click for a device or for a sensor to remove the respective object from your favorites.

For more information, see section Priority and Favorites 221.

More

KNOWLEDGE BASE

What options do I have to review my monitoring data in detail?

- https://kb.paessler.com/en/topic/90007

6.4 Sensor States

The color of a sensor or object indicates its status. In the table below, you find a list of states that a sensor or object can show. This list also reflects the priority of the sensor states whenever PRTG shows summarized sensor states, for example, in the device tree 164 or in geographical maps 3169. For example, if all sensors on a device show the Up status and one of the sensors changes to the Down status, the device shows the Down status as well because this status has a higher priority. The device is then displayed accordingly in the extended device tree views 174.

ⓘ The Down and Down (Partial) states are considered to be equal regarding status priority.

ⓘ In the device tree, hover over an object's name to view the total number of alarms for the object. In geographical maps, hover over over the location marker to view the total number of alarms at this location.

Status Icon	Status Name	Meaning
/	Down	At least one sensor on this object (or at this location) shows the Down status. ▪ PRTG is unable to reach the device or the sensor has detected an error. For more information, see section Sensor Behavior for the Warning and Down States 181. ⓘ In this case, the sensor does not record any data in its channels while it shows the Down status. ▪ There is an error limit in the channel settings 3121 or the sensor shows the Down status because of a lookup 3604. ⓘ In this case, the sensor continues to record data in all channels although it shows the Down status.
	Down (Partial)	In a cluster, at least one cluster node reports that this sensor shows the Down status, while at least one other cluster node reports that the same sensor shows the Up status. ⓘ This status is not available for sensors on remote probes in a failover cluster 128.
/	Down (Acknowledged)	At least one sensor on this object (or at this location) showed the Down status and a user acknowledged this status via Acknowledge Alarm in the context menu 226. ▪ There is no sensor in the Down status. ⓘ For acknowledged alarms, PRTG does not send further notifications 3173.

Status Icon	Status Name	Meaning
		ⓘ If you pause and resume a sensor in the Down (Acknowledged) status, it shows the Down status again.
W /	Warning	At least one sensor on this object (or at this location) shows the Warning status. ▪ The sensor detected an error and shows the Warning status but the sensor is trying to reach the target device again. The sensor might soon change to the Down status. For more information, see Sensor Behavior for the Warning and Down States 181. ▪ There is a warning limit in the channel settings or the sensor shows the Warning status because of a lookup. ▪ There is no sensor in the Down or Down (Acknowledged) status.
U /	Unusual	At least one sensor on this object (or at this location) shows the Unusual status. ▪ The sensor reports unusual values for this weekday and this time of the day. The unusual detection is based on the sensor's historic average data. You can configure or disable the unusual detection in the system administration settings under Monitoring 3309. ▪ You can also disable the unusual detection for specific groups. For more information, see section Group Settings 584. ▪ There is no sensor in the Down, Down (Acknowledged), or Warning status.
/	Up	All sensors on this object (or at this location) show the Up status. ▪ The last scan was okay and the sensors receive data. ▪ There is no sensor in the Down, Down (Acknowledged), Warning, Paused, or Unusual status.
/	Paused	All sensors on this object (or at this location) show the Paused status.

Status Icon	Status Name	Meaning
		▪ The sensor is paused for a specific time span, indefinitely, or because of a dependency 139. ▪ There is no sensor in the Down, Down (Acknowledged), Warning, Unusual, or Up status. ⓘ A sensor in the Paused status does not count towards the maximum number of sensors that your license allows.
? /	Unknown	All sensors on this object (or at this location) show the Unknown status. ▪ The sensor has not received any data yet or there is an error in (network) communication, likely on the probe system. If sensors continuously show this status, you might need to restart PRTG. For extended troubleshooting, see the Knowledge Base: What to check if sensors are gray? and My sensors show the Unknown status after a PRTG core server restart. What can I do? ▪ There is no sensor in the Down, Down (Acknowledged), Warning, Unusual, Paused, or Up status.

Sensor Behavior for the Warning and Down States

The Down status indicates that there is an issue with an object, for example, a device. There are various reasons for the Down status, for example, an interruption in the physical connection to the device or an internet connection outage.

After a failed request, PRTG tries to contact the device again before it sets a sensor to the Down status (this is true for almost all sensors):

1. If a request to a device fails for the first time, the sensor changes to the Warning status. PRTG repeats the request and immediately attempts to rescan the device.
2. If the second request also fails, the sensor changes to the Down status by default until the device is reachable again. You can change this behavior in the scanning interval 449 settings of any object in the device tree. PRTG tries to reach the device with every scanning interval.

This procedure gives devices and services the chance to recover from a momentary overload and prevents false alarms. Still, you are immediately informed about any network issues.

ⓘ This behavior does not apply to the Warning or Down states that result from warning limits or error limits in the channel settings. This behavior also does not apply to channels that use lookups.

More

KNOWLEDGE BASE

What to check if sensors are gray?

- https://kb.paessler.com/en/topic/25643

My sensors show the Unknown status after a PRTG core server restart. What can I do?

- https://kb.paessler.com/en/topic/87266

VIDEO TUTORIAL

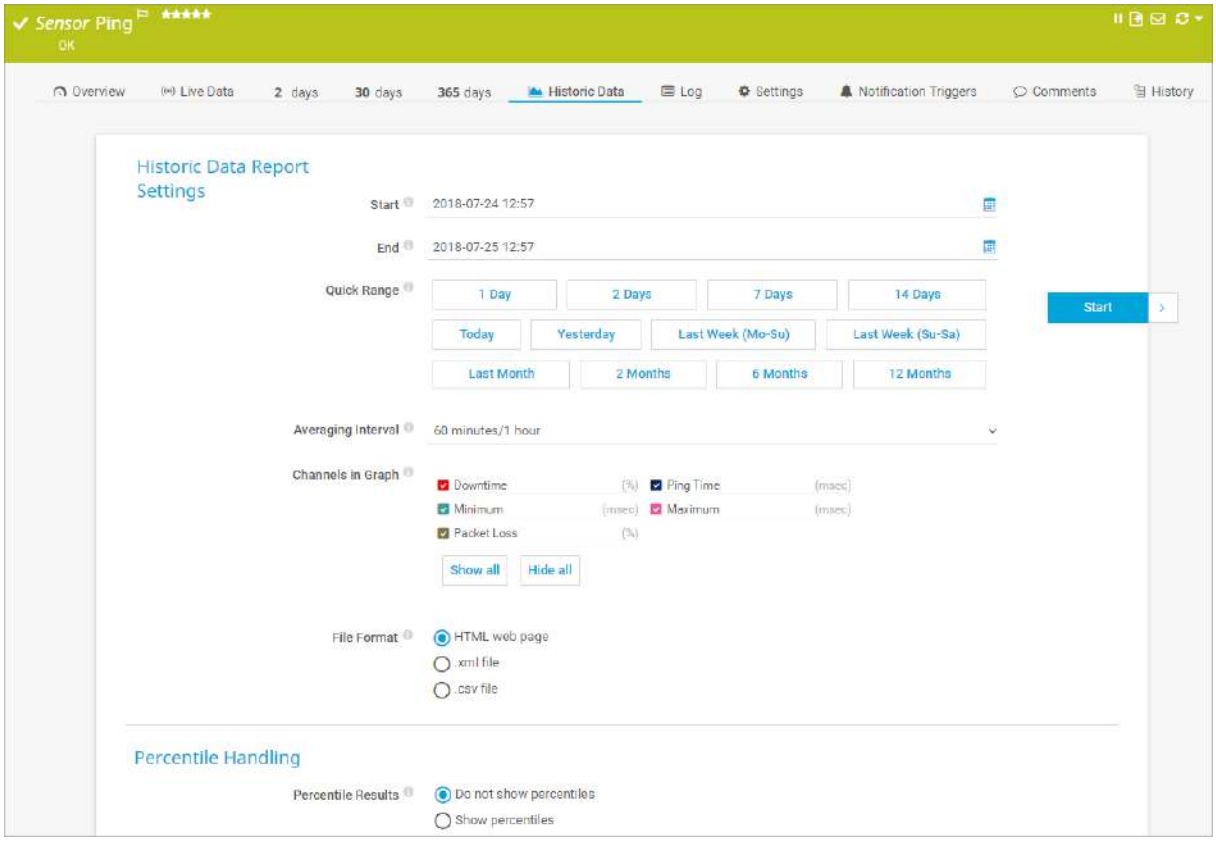
Sensor states

- https://www.paessler.com/support/videos-and-webinars/videos/sensor-states

6.5 Historic Data Reports

For quick reviews of a sensor's monitoring data, use historic data reports as an alternative to the comprehensive reports 3192 feature. You can run and view a historic data report for each sensor on demand. Additionally, you can export a sensor's historic data as an .xml file or a .csv file to your computer to further process the data with third-party applications.

There are two ways to open historic data reports: Either click the Historic Data tab of a sensor or select Sensors | View Historic Data from the main menu bar 251.



Historic Data Tab of a Ping Sensor

Historic Data (Sensor Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.

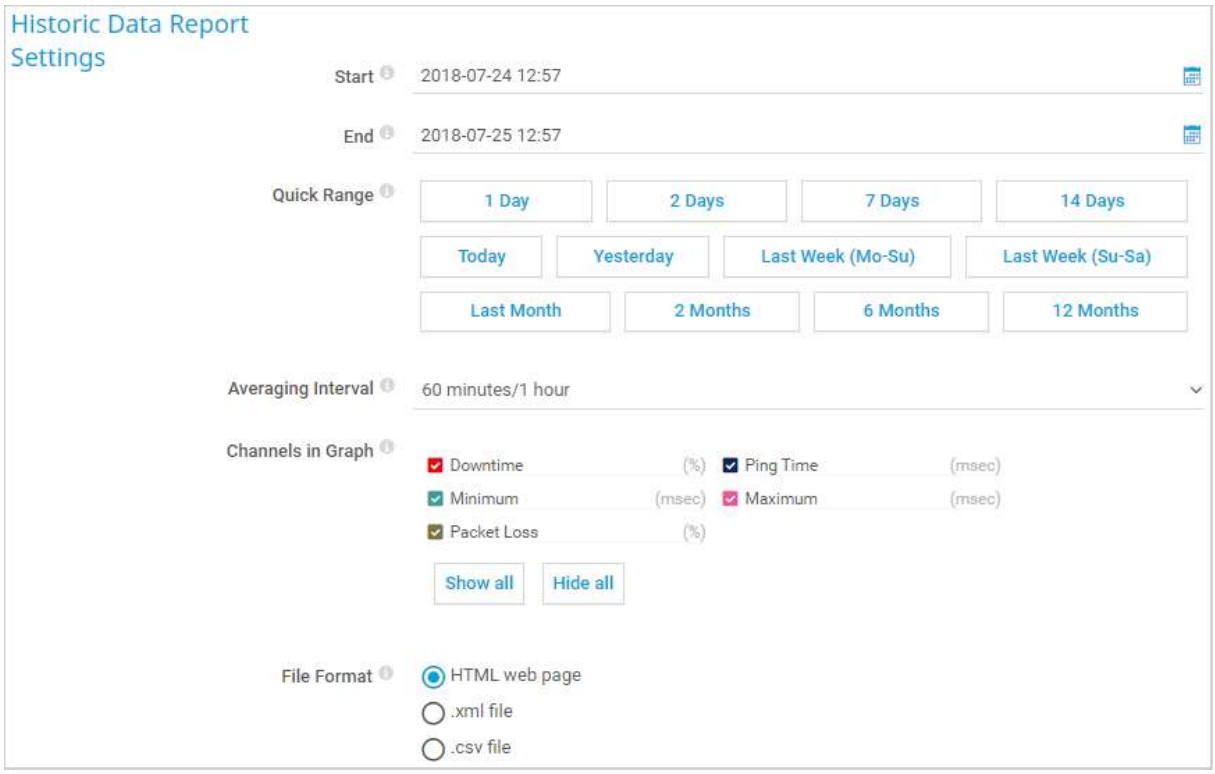
Tabs Bar for Sensors

The Historic Data tab is only available for sensors, not for probes, groups, or devices. When you open the Historic Data tab of a sensor, no sensor selection is available. If you want to select a different sensor for the report, select Sensors | View Historic Data from the main menu bar.

Historic Monitoring Data (Sensors Main Menu)

When you open historic data reports via Sensors | View Historic Data from the main menu bar, PRTG asks you to select the sensor for which you want to create a report with the object selector 219.

Historic Data Report Settings



Historic Data Report Settings

Setting	Description
Sensor	This setting is only visible if you open the View Historic Data option from the main menu bar. To select the sensor for which you want to create the report, click to open the object selector. For more information, see section Object Selector 219.
Start	Specify the start date and time for the data that you want to review. Use the date time picker to enter the date and time. You cannot generate the historic data report if monitoring data was deleted 3333 after the specified start date. Set the start of the report to a date for which data is available.
End	Specify the end date and time for the data that you want to review. Use the date time picker to enter the date and time.
Quick Range	You can use several buttons to select start and end dates more quickly. Click any of these buttons to change the Start and End values:

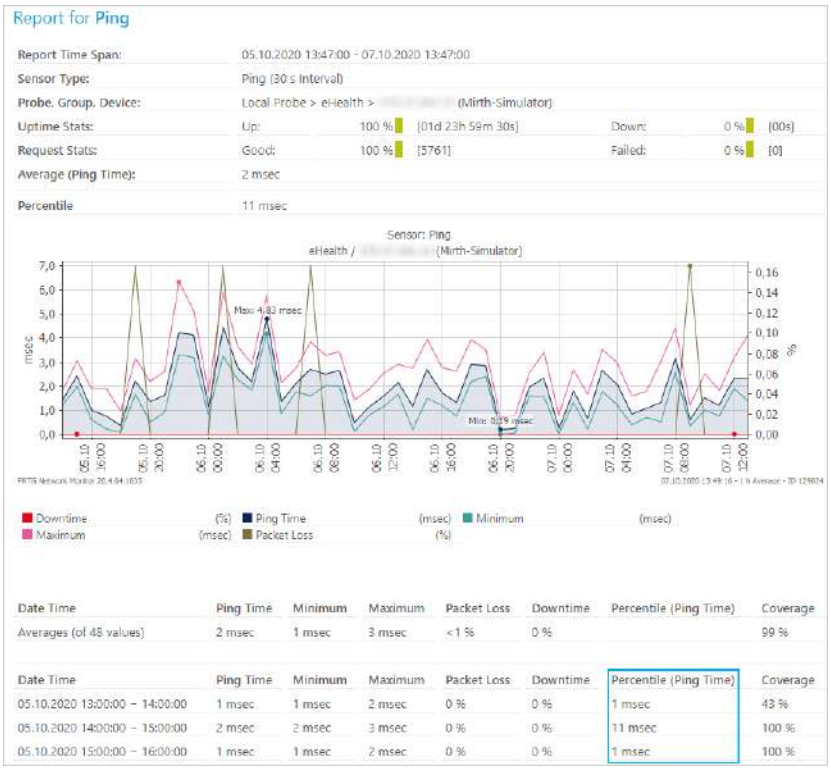
Setting	Description
	▪ 1 Day, 2 Days, 7 Days, or 14 Days: Set the date range 218 to the respective day or days. The current time of the current day is the end date. ▪ Today, Yesterday, Last Week (Mo-Su), Last Week (Su-Sa), Last Month, 2 Months, 6 Months, 12 Months: Set the date range to the last matching period. It starts at 00:00 and ends at 00:00 of the following day.
Averaging Interval	With this option, you can activate and configure averaging. Select an interval for which PRTG calculates the average value. You can choose from: ▪ No interval (display raw data): PRTG performs no averaging and displays only raw data. ⓘ PRTG stores raw data for up to 40 days. After this time, PRTG calculates averages again. ▪ 15 seconds, 30 seconds, or 60 seconds/1 minute ▪ 2 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes, or 60 minutes/1 hour ▪ 2 hours, 4 hours, 6 hours, 12 hours, or 24 hours/1 day ⓘ A shorter interval results in a more detailed historic data report for the sensor. The best settings for you depend on the scanning interval of the sensor, the selected time period, and the intended use for the historic data report. Try different settings and compare the results. See also Automatic Averaging 188 in this section.
Channels in Graph	This setting is only visible if you view historic data via the Historic Data tab of a sensor. Select the channels that you want to include in the graph of the historic data report. You can select individual channels via the respective check boxes, and show or hide all channels via the Show all or Hide all buttons. In the graph, PRTG then only shows the data of selected channels. ⓘ The historic data report table always shows the data of all channels.
Cluster Node	This setting is only visible if the sensor runs on a cluster probe. Select the cluster node's data that PRTG includes in the historic data report: ▪ All nodes: Include the data of all cluster nodes in the report. ▪ [Several specific nodes]: Use a specific cluster node's data for the report. The cluster nodes you see are specific to your setup.
File Format	Select the output format for the report:

Setting	Description
	▪ HTML web page: Display the result directly as an HTML web page. This is also a good option if you want to check the results before you export them to a different file format. ▪ .xml file: Export the data as an .xml file. Your browser usually shows a download dialog when you use this option. ▪ .csv file: Export the data as a .csv file, for example, to import it into Microsoft Excel. Your browser usually shows a download dialog when you use this option.

Percentile Handling

Percentile Handling

Setting	Description
Percentile Results	Define if you want to include an additional percentile calculation 3618 of your data in the historic report: ▪ Do not show percentiles: PRTG does not use a percentile formula to calculate your monitoring results. It only shows the standard values.

Setting	Description
	▪ Show percentiles: PRTG displays an additional percentile calculation for the primary channel in the value table for each scanning interval.  Example of a Historic Data Report w ith Percentile Calculation for the Primary Channel
Percentile Type	This setting is only visible if you enable Show percentiles above. Enter the percentile type that you want PRTG to use for the calculation. If you choose, for example, to calculate the 95th percentile, enter 95 here and 5% of peak values are discarded. Enter an integer.
Percentile Averaging Interval	This setting is only visible if you enable Show percentiles above. Enter a value to define the averaging interval on which PRTG bases the percentile calculation. The default value is 300 seconds (5 minutes). This means that PRTG takes 5-minute averages as basic values for the percentile calculation. Enter an integer.
Percentile Mode	This setting is only visible if you enable Show percentiles above. Select the mode for percentile calculation: ▪ Discrete: PRTG takes discrete values to calculate percentile results. ▪ Continuous: PRTG interpolates between discrete values and bases the calculation on interpolated values.

Click Start to generate a historic data report.

You cannot generate the historic data report if monitoring data was deleted 3333 after the specified start date. Set the start of the report to a date for which data is available.

Remarks for Reports

- Any sensor graph in your report only shows channels that you enable via the Show in graphs option in the channel settings 3121.
- Reports show statistics for the uptime (the Up and Down states 179 in percent) and for requests (Good and Failed in percent). PRTG rounds values between 5% and 95%, as well as 100% and 0%, to whole numbers without decimal places. Other values are shown with 3 decimal places.
- Because PRTG rounds values, the statistics in the report section Sensor Status History can differ from the values in the report section Uptime Stats by a few seconds.
- PRTG limits data reporting to 5 requests per minute.
- Reports cannot show uptime or downtime data for the Sensor Factory sensor.
- Create reports that include an appropriate amount of data. Reports might not work as expected if PRTG has to process too many sensors with short scanning intervals. Adjust your report size and the time span that the report covers, if necessary.

Automatic Averaging

For performance reasons, PRTG automatically averages monitoring data when it calculates data for large periods of time.

Period of Time in Report	Minimum Level of Detail (Averaging Interval)
Up to 40 days	Any
40 to 500 days	60 minutes/1 hour or longer

Reports for periods that are longer than 500 days are not possible. If you enter a longer period, PRTG automatically shortens it to 365 days.

In some cases, the generated report might contain a period of time that differs from the defined start and end date for the report because of internal averaging processes. When averaging intervals are longer than 1 hour and do not equal 24 hours, and when they are combined with specific periods of time, the resulting data points might be asynchronous to the periods of time. Consider this behavior particularly if you use application programming interface (API) calls 3511 to generate reports.

More

KNOWLEDGE BASE

Why is there missing data in historic data reports?

- https://kb.paessler.com/en/topic/61382

How does PRTG compute CPU Index, Traffic Index and Response Time Index?

- https://kb.paessler.com/en/topic/313

6.6 Similar Sensors

With PRTG, you can detect relationships between different components in your network. For example, you can detect extraordinarily high CPU load that correlates with extraordinarily high traffic at a specific time of a day or week. This can give you a hint to further investigate that part of your network.

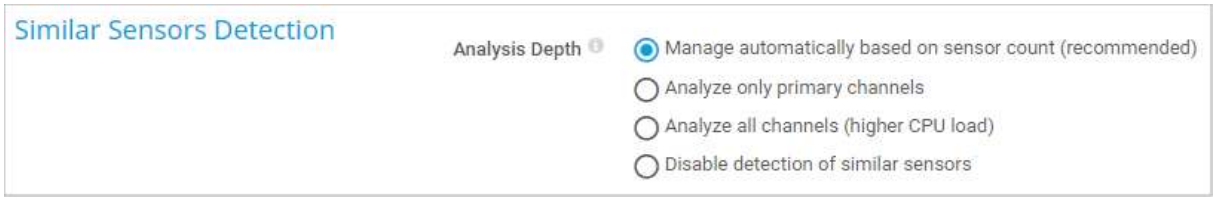
What Is Similarity?

The similarity calculation is based on the values that are saved in the sensor history. If measured values change in the same way, the Similar Sensors Detection feature detects it and shows you the sensors for which it found similar data relations. PRTG shows all sensors that reach 85% to 100% similarity.

The analysis of similar sensors is a heuristic calculation that shows interconnections and correlations in your network. The analysis is completely automated. It is based on mathematics and fuzzy logic and optimizes your sensor usage by tracking redundant monitoring of some aspects of your system.

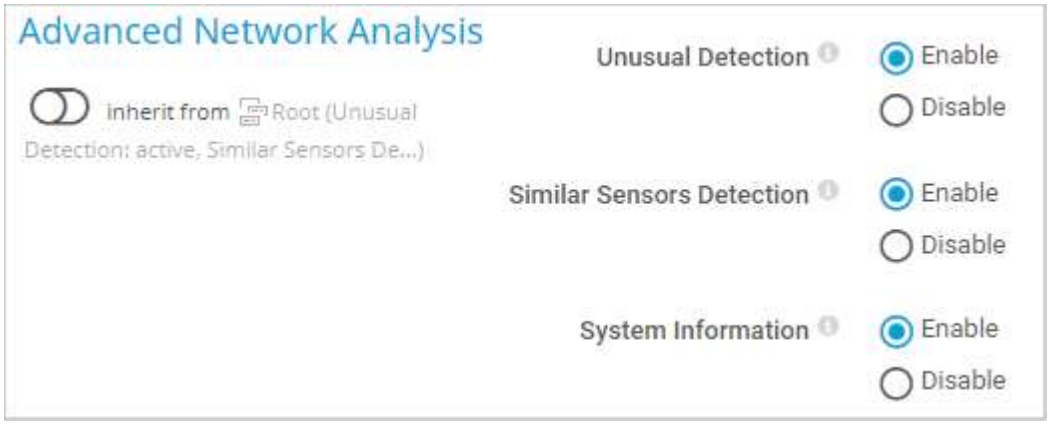
Similar Sensors Detection

You can adjust the depth of the similar sensors detection or turn it off under Setup | System Administration | Monitoring.



Similar Sensors Detection Settings

You can also enable or disable the similar sensors detection for specific probes, groups, and devices, and specify inheritance 135 in the object's settings 198, section Advanced Network Analysis.



Activation of the Similar Sensors Detection

There are two options to view similar sensors:

- Via the Overview tab of sensors that includes a Similar Sensors section 190 where PRTG lists channels that show similarities to channels of the selected sensor.
- Via Sensors | Simulate Error Status in the main menu bar where you get an overview 191 of all similar sensors.

To edit the list of similar sensors results, use the available filters 192.

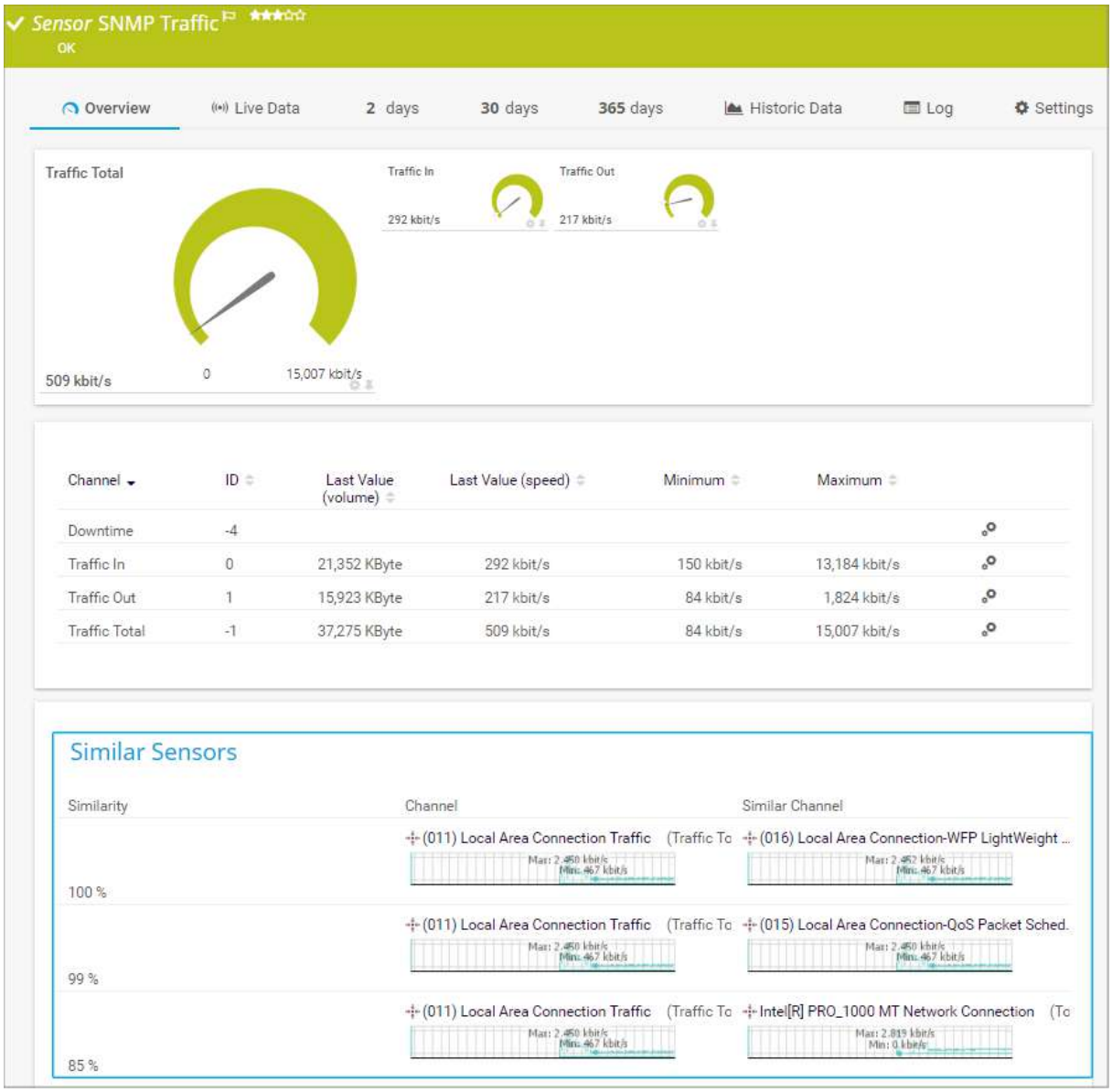
Similar Sensors (Sensor Overview Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.

Tabs Bar for Sensors

On the Overview tab of a sensor, PRTG lists channels that show similarities to channels of the selected sensor. The table is empty if PRTG detects no similarities to the selected sensor.

ⓘ PRTG shows similar sensors here when channels have 85% similarity or more. The similar sensors detection saves up to 15 entries per sensor.

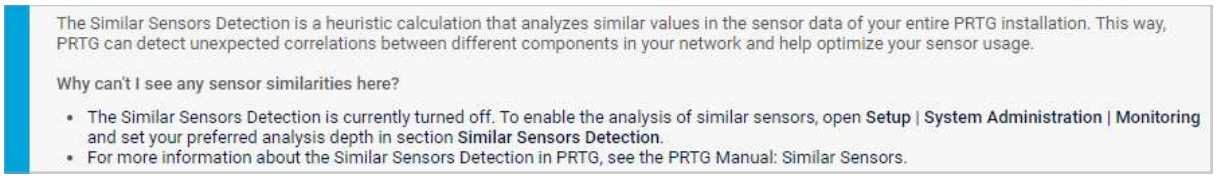


Similar Sensors Section on a Sensor's Overview Tab

The Similar Sensors section provides the following information.

Column Header	Description
Similarity	Shows the similarity between two channels in percent.
Channel	Shows a channel of the selected sensor.
Similar Channel	Shows a channel of a sensor that is similar to the channel of the selected sensor that you can see in the Channel column in the same row.

ⓘ PRTG does not show the Similar Sensors section when the analysis is disabled or when you exceed 1,000 sensors and select the Manage automatically based on sensor count (recommended) option as Analysis Depth in the Monitoring 331 settings. In this case, you see the following notice:


The Similar Sensors Detection is a heuristic calculation that analyzes similar values in the sensor data of your entire PRTG installation. This way, PRTG can detect unexpected correlations between different components in your network and help optimize your sensor usage.

Why can't I see any sensor similarities here?

- The Similar Sensors Detection is currently turned off. To enable the analysis of similar sensors, open **Setup | System Administration | Monitoring** and set your preferred analysis depth in section **Similar Sensors Detection**.
- For more information about the Similar Sensors Detection in PRTG, see the PRTG Manual: Similar Sensors.

Similar Sensors Detection Notice

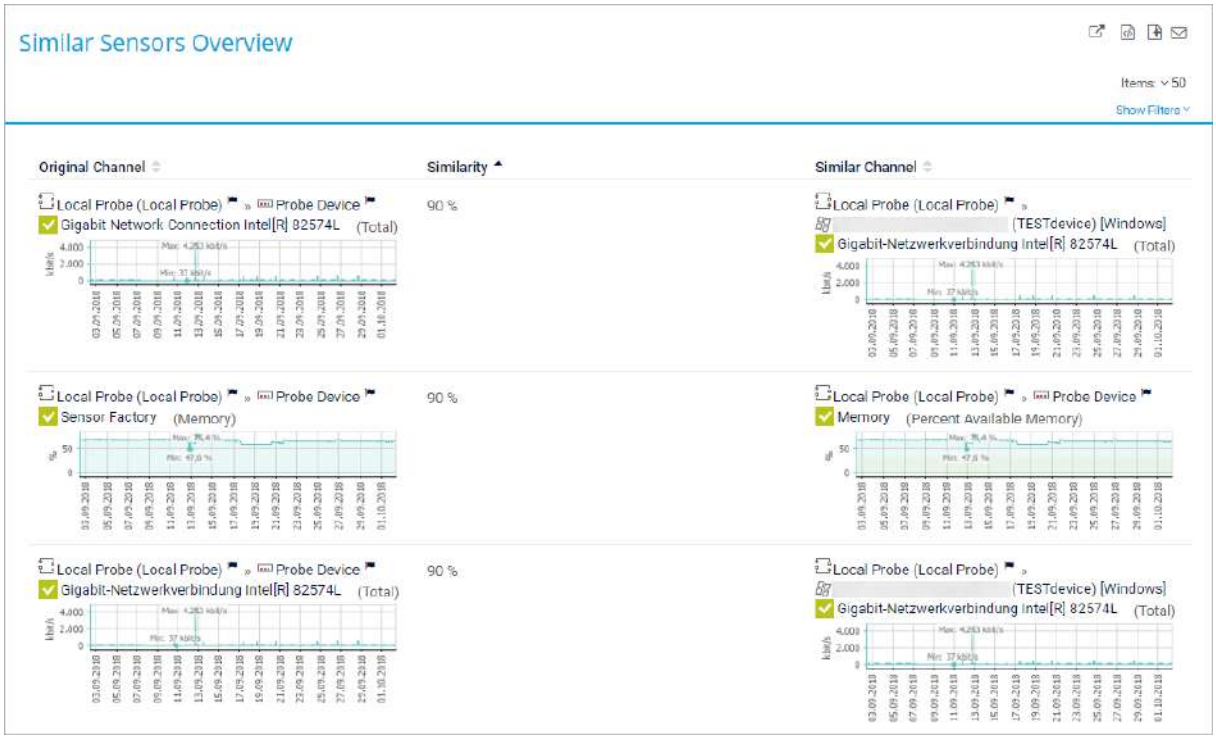
Similar Sensors Overview (Sensors Menu)

This page shows the results of the similar sensors detection from the entire monitoring database. PRTG lists all channels with similarities here. Above the table, there are several filter options to display similar sensors as required. Select the object of interest, the degree of similarity, and display back references.

For more information, see also section Working with Table Lists 216.

ⓘ The analysis of similar sensors requires sensor data from at least seven days to have enough data for comparison. If not enough data is available, no data is shown on the Similar Sensors Overview or in the Similar Sensors section on a sensor's Overview tab.

ⓘ PRTG shows similar sensors here when channels have at least 85% similarity. Furthermore, the analysis saves up to 15 entries per sensor.



Similar Sensors Overview

You can click the column headers to sort the list. The Similar Sensors Overview provides the following information.

Column Header	Description
Original Channel	Shows channels that other channels are compared to. Click the column header to sort the list according to the order in the device tree in ascending or descending order.
Similarity	Shows the similarity between two channels in percent. Click the column header to sort the list according to the similarities in ascending or descending order.
Similar Channel	Shows a channel that is similar compared to the original channel. Click the column header to sort the list according to the order in the device tree in ascending or descending order.

ⓘ PRTG does not show the Similar Sensors Overview item in the main menu bar if you disable the analysis or if you exceed 1,000 sensors and select the Manage automatically based on sensor count (recommended) option as Analysis Depth in the Monitoring 3311 settings.

Adjust the Similar Sensors Overview to Your Needs

You can use various filters to adjust the results in the Similar Sensors Overview. Click Show Filters and edit the filters that appear.

Filters for the Similar Sensors Analysis

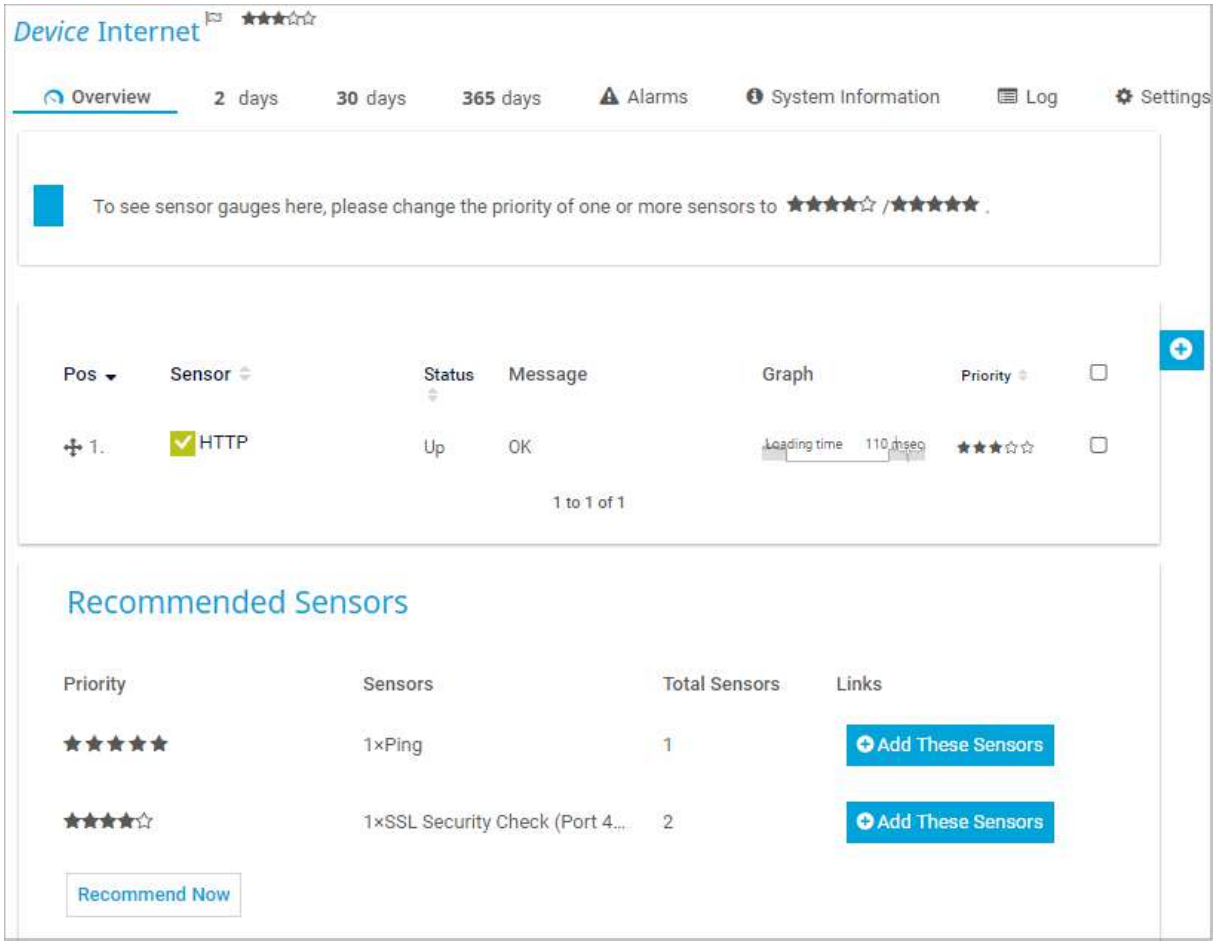
Filter	Description
Filter By Object	Select the device, probe, or group that you want the Similar Sensors Detection to cover. This way, you can apply the analysis to the parts of your network that you are interested in.
Filter By Maximum Similarity	Select a degree of similarity from 85% to 100%.
Inverted Relationships	If you select Show, PRTG shows all similarity relationships, that is, A matches B and B matches A. If you select Hide, PRTG only shows A matches B relationships. This reduces the number of displayed similar sensors.

6.7 Recommended Sensors

With the Recommended Sensors Detection feature, PRTG can explore any device and check which sensors you have already created. If it finds useful sensors that you have not created yet, you see a list of recommended sensors for your device.

You cannot use this feature on the hosted probe of a PRTG Hosted Monitor instance. You can use this feature on remote probes.

The recommended sensors detection does not apply to the user group setting 3347 Allowed Sensors. Therefore, read/write users can also add all recommended sensors.



Recommended Sensors on Device Overview Tab

Get Sensor Recommendations

By default, PRTG recommends sensors for any device that you add and shows the suggested sensors for the device on its Overview tab, as long as your installation includes less than 5,000 sensors in total. To add the recommended sensors, click Add These Sensors.

You can see the time that has passed since the last sensor recommendation in the page header bar 170 on the Overview tab of a device.

If you want to manually start the recommended sensors detection on any device, follow the steps below.

Step 1: Select the Device

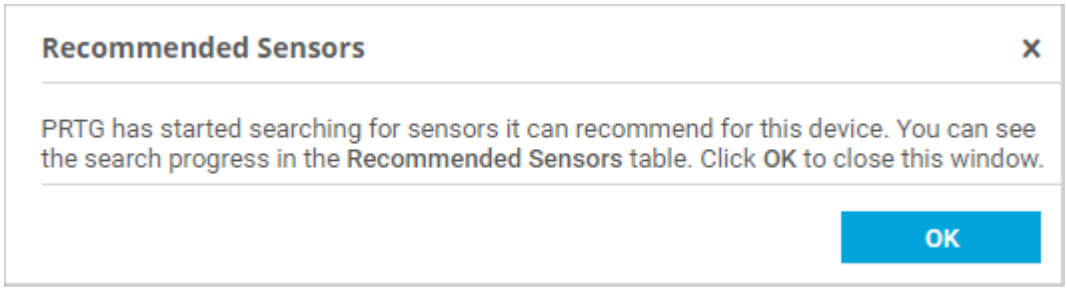
Open the Overview tab of the device that you want to analyze.

Step 2: Recommend Now

To start the analysis of your device, click Recommend Now or right-click the device and select Recommend Now from the context menu 234.

ⓘ If you do not see the Recommend Now option, make sure that the Recommended Sensors Detection in the Monitoring 3312 settings. Probe devices do not support this option.

Depending on the complexity of your device, it can take some time until you see the results of the analysis.



Recommended Sensors Investigation

PRTG runs the recommended sensors detection with low priority in the background to prevent potential performance issues. Because of this, the recommended sensors detection can take more time than expected if PRTG needs resources to ensure the gapless monitoring of your network. By default, the recommended sensors detection starts automatically when you add a new device, when you do not have more than 5,000 sensors, or when the last analysis was executed more than 30 days ago. You can change these settings under Setup | System Administration | Monitoring, section Recommended Sensors Detection.

ⓘ To recommend Simple Network Management Protocol (SNMP) sensors 3683 for a device, the detection engine uses the SNMP version that you defined in the Credentials for SNMP Devices section of the device settings 603.

Step 3: Get the Results

After PRTG analyzed your device, it suggests a list of sensors that are useful for a more comprehensive monitoring.

List of Recommended Sensors

The list of recommended sensors provides the following information.

Column Header	Description
Priority	Shows which priority 221 the suggested sensors have when you add them. The recommended sensors table is sorted by priority, beginning with the top priority (★★★★★) in the first row. ⓘ You can manually change the priority of a sensor after you add it.
Sensors	Shows the suggested sensors and the number of sensors of one type that PRTG recommends for this device. For example, you might want to add an SNMP Traffic sensor multiple times for several network interfaces.
Total Sensors	Shows the total number of suggested sensors per table row. These sensors have the same priority.
Links	Displays an Add These Sensors button for every table row. Click to automatically add the sensors in this table row to the device.

ⓘ The recommended sensors detection checks if a certain sensor exists on your device and recommends that you add this sensor if it does not exist. If this sensor existed previously on the device, but you deleted it, PRTG suggests this sensor again. In this case, ignore the recommendation of this sensor or follow step 4 196.

Step 4: Add Recommended Sensors

Click Add These Sensors in a table row to add all sensors in this row to the analyzed device.

ⓘ If you want to add all suggested sensors regardless of their priority, click every Add These Sensors button in the Recommended Sensors table. If you want to add only some of the sensors of a certain priority, click Add These Sensors, then delete 240 or pause 224 the sensors you do not need afterward.

Settings for the Recommended Sensors Detection

You can also adjust the settings for the recommended sensors detection or disable it under Setup | System Administration | Monitoring.

Recommended Sensors Detection Settings

If you use the Manage automatically based on sensor count (recommended) setting, PRTG uses an intelligent assistant to count the number of sensors you have and decides whether to start the detection of recommended sensors or not. The detection does not start if your PRTG installation includes 5,000 sensors or more to prevent performance issues. We recommend that you use this option so that you do not miss any important monitoring data about your network and so that you do not risk performance issues.

ⓘ Disable the recommended sensors detection if you encounter performance issues or if you do not want to display this information on device Overview tabs.

Auto-discovery

You can also use the auto-discovery to find suitable sensors. You can start the auto-discovery when you add a new device 370, you can manually start 265 it at any time, or you can choose if you want PRTG to analyze a whole section 592 of your network, for example, devices that are covered by a certain IP address range.

ⓘ The auto-discovery has a higher priority than the detection of recommended sensors. If both are active, PRTG queues the sensor recommendation and executes the auto-discovery first.

6.8 Object Settings

Probe, group, device, and sensor pages have tabs that you can use to navigate between different options. For example, you can view your network's status, view monitoring results, or change settings.

Tabs Bar for Sensors

General Settings

On the Settings tab, you can define all settings for the selected object. The available options vary depending on the kind of object that you select. See the following sections for information about the object types:

- Root Group Settings 419
- Probe Settings 457
- Group Settings 520
- Device Settings 588
- Sensor Settings

ⓘ You cannot open channel settings 3121 via tabs. Go to a sensor's Overview tab to edit the channel settings.

Notification Triggers Settings

On the Notification Triggers tab, you can set notification triggers for every object. If you use these settings for a probe, group, or device, they are inherited to all sensors on these objects. The available notification trigger options are the same for all objects.

For more information, see section Notification Triggers Settings 3133.

Comments

On the Comments tab, you can enter free text for each object. You can use this function for documentation purposes or to leave information for other users.

History

On the History tab, all changes in the settings of an object are logged with a time stamp, the name of the user who made the change, and a message. The history log retains the last 100 entries.

ⓘ On some pages, you can click in the page header bar 170 to access the history of subordinate objects. This includes system administration 3293 settings and account settings 3238, reports 3192, libraries 3176, and maps 3214. For more information, see section Logs 208.

6.9 Alarms

The alarms list shows all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. Sensors in the Up, Paused, or Unknown states do not appear here.

ⓘ By default, table lists 216 that show alarms are sorted by priority 221. Click a column header to sort the list items by a different category.

Alarms List

There are two ways to display the alarms list. Either click the Alarms tab of a probe, group, or device, or click Alarms in the main menu bar 247.

Alarms (Object Tab)

Probe, group, device, and sensor pages have tabs that you can use to navigate between the different options. For example, you can view your network's status, view monitoring results, or change settings.

Tabs Bar for Groups and Probes

Click the Alarms tab of a probe, group, or device to show a table list of all sensors on the selected object that show the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status 179. This list is a subset of the entries that are available via the Alarms | All option in the main menu bar.

ⓘ The Alarms tab is not available for sensors.

Alarms (Main Menu Bar)

Click Alarms in the main menu bar to show a table list of all sensors in your installation that show the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. You can also show these sensors as gauges or only show a subset of sensors in specific states. Hover over Alarms to show further options:

Option	Description
All	Open a list of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status.
Show as Gauges	Open a page with the gauges of all sensors that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status. The size of the gauges corresponds to the sensor's priority.
Errors Only	Open a list of all sensors that are in the Down, Down (Partial), or Down (Acknowledged) status.
Warnings Only	Open a list of all sensors that are in the Warning status.
Unusuals Only	Open a list of all sensors that are in the Unusual status.

Acknowledge Alarm

An acknowledged alarm shows the Down (Acknowledged) status. It does not trigger 313 any more notifications 317.

ⓘ If the alarm condition clears, the sensor usually returns to the Up status with the next sensor scan.

ⓘ If a sensor in the Down (Acknowledged) status was paused and resumed, it shows the Down status again.

To acknowledge an alarm, right-click a sensor that shows the Down status. From the context menu 226, select Acknowledge Alarm, then select a time span, optionally enter a message, and click OK. The message appears in the last message value of the sensor.

The time spans that you can select are: Acknowledge Indefinitely, acknowledge For 5 Minutes, For 15 Minutes, For 1 Hour, For 3 Hours, For 1 Day, or Until. If you select Until, provide the following information:

Field	Description
Selected Objects	Shows the sensors for which you want to acknowledge the alarm. You can acknowledge alarms for more than one sensor using multi-edit 315.
Message	Enter a text, for example, the reason why you acknowledge the alarm. Enter a string or leave the field empty.
Until	Select the date when the Down (Acknowledged) status ends. Use the date time picker to enter the date and time.