14.4 Channel Definitions for Flow, IPFIX, and Packet Sniffer Sensors

With custom Flow sensors, custom IPFIX3441, or custom Packet Sniffer sensors3439, you have the option to provide a Channel Definition with the following syntax, one entry per channel:

```
#<id>:<Name>
<Rule>
```

Syntax

- The <id> must be 1 or a higher number, and it must be unique for the sensor. This means that each channel definition must have a unique ID.
  The maximum channel ID that you can use is 2147483648 (2^31). PRTG does not support higher IDs. We recommend that you use channel IDs like 1, 2, or 3.
- The <id> is linked to the historic data.
  As soon as you change the ID, you lose the history for the channel that the ID was linked to.
- One rule can span multiple lines.
- The next rule starts with a # as the first character in a line.
- The <name> is the display name of the channel.
- PRTG processes the rules from top to bottom (the number does not matter) and accounts the data to the first match.
- PRTG automatically adds one channel named Other. This channel counts all traffic for which you do not define a specific channel.
- After the name, you can use an optional [<unit>] to override the automatic unit, which is based on the source sensor.

The <Rule> syntax is identical to the one described in section Filter Rules for Flow, IPFIX, and Packet Sniffer Sensors3596. Because PRTG accounts data to the first match, make sure that you start with the most specific rule at the top and get less specific towards the bottom.

We recommend that you write the rules list in an external editor first and then paste it into the Channel Definition field of the sensor. If the rules contain an error, PRTG removes the entries after you add them.

You cannot delete channels even if you remove a channel from the channel definition. You also cannot change the display name of channels using the channel definition of custom flow sensors. You can only rename channels in the channel settings3121.

Example

General example:

```
#5:HTTP
Protocol[TCP] and
(SourcePort[80] or DestinationPort[80] or SourcePort[8080] or
DestinationPort[8080])
```

Channel definition example for differentiating by protocol:

```
#1:TCP
Protocol[TCP]

#2:UDP
Protocol[UDP]

#3:ICMP
Protocol[ICMP]
```

More

KNOWLEDGE BASE

How can I change the default groups and channels for flow and Packet Sniffer sensors?

- https://kb.paessler.com/en/topic/60203

14.5 Define IP Address Ranges

In some setting fields, you can either enter a host name or a single IP address, or you can define IP address ranges. These are available, for example, for Flow and Packet Sniffer sensors 3683 and for probe connection settings 3327. PRTG follows a common syntax for IP address ranges.

For the supported syntax of the automatic network discovery feature in PRTG, see section Add an Auto-Discovery Group 277.

Available Options

Option	Description	Syntax	Examples
Simple	Enter a fixed IP address.	a.b.c.d	10.0.10.9
Hostname	Enter a hostname. PRTG resolves it to an IP address in your network.	hostname	device-xyz
Hostmask	Enter a hostmask. A hostmask defines the relevant bits of the IP address. Valid hostmasks are /0 - /32 for IPv4 and /0 - /128 for IPv6.	a.b.c.d/h or a.b.c.d/e.f.g.h	10.0.0.0/24
Range	Enter an IP address range. Replace each letter of a, b, c, d with either ▪ * (asterisk) for any value; corresponds to 0-255 or ▪ x-y for any range between 0 and 255.	a.b.c.d	10.0.0.1-20 or 10.*.0.* or 10.0.0-50.*

14.6 Define Lookups

PRTG uses lookups for some sensors and for other sensors that have custom channels. In general, lookups map status values as returned by a device (usually integers) to more informative expressions in words. Additionally, lookups can define a sensor status [179] based on the status value returned by a device, just like channel limits [3122] can define a sensor status. For a printer that returns the status value 1, for example, PRTG can show a sensor in the Warning status with the text message Toner Low instead of only displaying the status value 1.

You can customize lookups by defining your own text messages that a channel shows and by mapping them to a certain sensor status. See section Customizing Lookups [3611].

If a channel uses lookups, you can individually define how to control the status of the sensor, either by using the lookup definition or by using limits for numeric values returned by the device. For details, see section Channel Settings [3122]. It is not possible to use both definitions at the same time.

ⓘ Lookups do not change data in the PRTG database, they merely change the way a sensor shows a channel. Any change to lookup definition files applies to historic data as well as to live data.

ⓘ Some exceptions apply to the SNMP Custom String Lookup sensor that basically does an inverse lookup. It does not map an integer to a text message but only looks for matching strings in the lookup definition and shows a status based on this text value.

☁ To upload customized lookups to PRTG Hosted Monitor, see section Manage a PRTG Hosted Monitor Subscription.

In this section:

Requirement: Channel Unit "Custom"

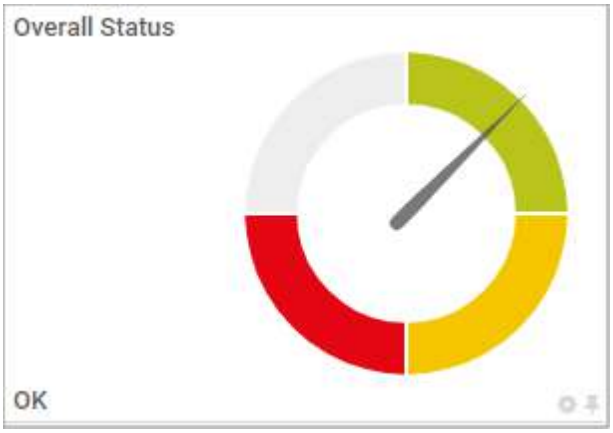
All channels with an enabled Lookup need to use the Channel Unit "Custom". For details, see section Channel Settings [3122].

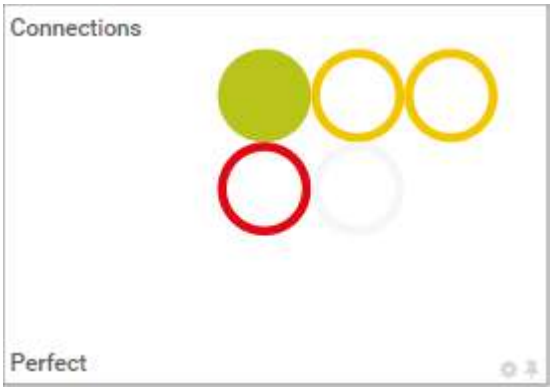
ⓘ There are sensors that provide the Channel Unit "Lookup" in their settings. Do not use the Channel Unit "Custom" for channels of these sensors if you want to use lookups. This results in malfunctioning lookup definitions. For the following sensors, select the Channel Unit "Lookup" in the settings and select the lookup file directly under Channel Lookup during sensor creation:

- Microsoft SQL v2
- MySQL v2
- Oracle SQL v2
- PostgreSQL
- SNMP Custom Advanced
- SNMP Custom Table

Visualization of Lookup Channels

PRTG can display channels that use lookups as follows.

Lookup Type	Visualization	Example
SingleInt, Range	Gauge	 A Gauge Showing the Status of a Lookup Channel
Boolean	Switch	 A Switch Showing the Status of a Boolean Lookup Channel

Lookup Type	Visualization	Example
BitField	Toggles	 Toggles Showing the Status of a BitField Lookup Channel

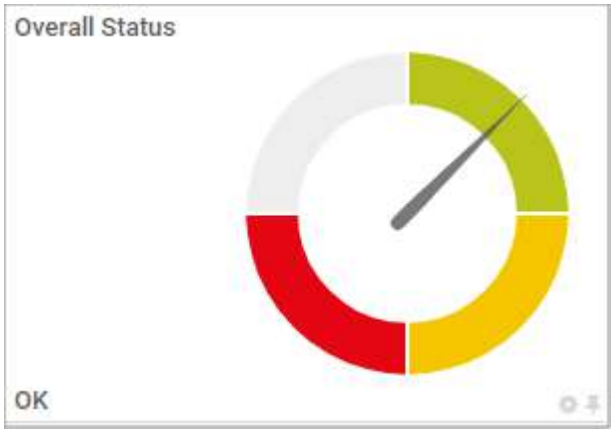
You can view the text messages for the different lookup values by hovering over the respective section.

Gauge Showing the Respective Lookup Message when Hovering over a Color Section

To see which lookup value in which channel shows the Warning or Down status, check the sensor message on a sensor's Overview tab:

Sensor Message on the Overview Tab

ⓘ We recommend that you stay below 120 lookup values to display visually informative gauges for primary channels. Non-primary channels have an upper limit of around 40 lookup values for gauges.



Gauge Showing 120 Lookup Values

The various sensor states that are displayed in gauges always follow the clockwise order Up < Warning < Down < Unknown. This order stays the same, no matter which numeric value you map to which sensor status in the lookup definition. See the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
  <ValueLookup id="example.lookups" desiredValue="1" undefinedState="olsWarning"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
    <Lookups>
      <SingleInt state="Ok" value="1">
        Works
      </SingleInt>
      <SingleInt state="Ok" value="2">
        Works a bit
      </SingleInt>
      <SingleInt state="Warning" value="4">
        Is slow
      </SingleInt>
      <SingleInt state="Error" value="8">
        Does not work
      </SingleInt>
      <SingleInt state="Ok" value="16">
        Works sometimes
      </SingleInt>
    </Lookups>
  </ValueLookup>
```

Even though the value 8 comes before the value 16, PRTG displays the state OK (shown as the Up status) before the state Error (shown as the Down status).

See Lookups Directory and Format 3608 and The XML Schema 3608 for more information about the lookup code and format.

Lookups Directory and Format

Lookups are defined in Extensible Markup Language (XML) format in files that end with .ovl. PRTG standard lookup files are located in the \lookups subfolder of the PRTG program directory 3636. PRTG maintains these files. In each of the files, lookups for one or more sensors are defined. Furthermore, the \lookups subfolder contains the \custom subfolder to store your customized lookups.

For a list of all standard lookup files, see section List of Standard Lookup Files 3786.

The files follow a basic principle. For each numeric value, you can define:

- A message that the sensor looks up and shows instead of the numeric value.
- The status that the sensor shows.

Use the SNMP Custom String Lookup sensor to map a string to a corresponding status. For this purpose, use the lookup type 3613 SingleInt.

You cannot access this directory on PRTG Hosted Monitor instances.

The XML Schema

An exemplary schema of the .xml files that contain the lookup definitions can look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="..." desiredValue="..." undefinedState="..." xmlns="..." xsi="...">
	<Lookups>
		<SingleInt state="..." value="...">status text</SingleInt>
		<SingleInt state="..." value="...">status text</SingleInt>
		<SingleInt state="..." value="...">status text</SingleInt>
	</Lookups>
</ValueLookup>
```

Element	Description	Attributes, Value Assignment, and Content
<?xml> content	This is the XML declaration that every .xml file begins with.	▪ version and encoding are 1.0 and UTF-8 respectively ▪ content: <ValueLookup>contentValueLookup</ValueLookup>

Element	Description	Attributes, Value Assignment, and Content
<ValueLookup> contentValueLookup </ValueLookup>	Defines the ID of the channel, which desiredValue is used, the status for undefined values (undefinedState), and links to the predefined schema definitions in PRTG that allow you to edit lookup files with supported editors.	▪ id: Specifies how the name of the lookup file is shown in the channel settings 3121. ⓘ PRTG parses the id as a lowercase string. ▪ desiredValue 3612: Contains the value that PRTG uses for the calculation of the Coverage. ▪ undefinedState: Optionally define a status for values that are not defined in the lookup file. If the target device returns a value that is not included in the lookup definition, the sensor shows this status (Ok, Warning, Error, or None) with an according message. Without a definition of undefinedState, the sensor only shows the returned value. ▪ xmlns:xsi/xsi: Refers to predefined XML schema definitions in PRTG that allow you to edit lookup files with supported editors. ▪ contentValueLookup: Lookup definitions <Lookups>contentLookups</Lookups>
<Lookups> contentLookups </Lookups>	Defines the particular lookups for the sensor data.	• contentLookups: One or more lookup entries, see below.
<SingleInt> status text </SingleInt> <Boolean> status text </Boolean> <BitField> status text </BitField>	Each element defines one lookup entry. There can be one or more lookup entries from the same lookup type 3613. ⓘ You can use only one kind of lookup type in one lookup file. This means only SingleInt, only Boolean, only BitField, or only Range. Different lookup types in one file are not allowed.	▪ state: Defines the status that the sensor shows. Allowed values are Ok, Warning, Error, and None. None does not trigger a status change. ⓘ State values must be capitalized for the sensor to work properly.

Element	Description	Attributes, Value Assignment, and Content
<Range> status text </Range>	The notation for the different lookup types can vary: ▪ <SingleInt state="..." value="...">status text</SingleInt> ▪ <Boolean state="..." value="...">status text</Boolean> ▪ <BitField state="..." value="...">status text</BitField> ▪ <Range state="..." from="..." to="...">status text</Range>	▪ value: Defines the value that triggers the lookup. Enter an integer. Range always needs both values "from" and "to". ▪ status text: Defines a status text that PRTG uses as substitution text and shows instead of the integer, for example, a status message. The SNMP Custom String Lookup sensor maps the status text to one of the specified states. For this sensor, use SingleInt.

Because all .xml files that contain lookup definitions are delivered in a previously specified schema as indicated above, you can customize lookups[3611] accordingly.

Example

The following code illustrates the lookup definition for the toner status of the SNMP HP LaserJet Hardware sensor:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
	<Lookups>
		<SingleInt state="Ok" value="0">Toner Okay</SingleInt>
		<SingleInt state="Warning" value="1">Toner Low</SingleInt>
		<SingleInt state="Error" value="2">No Toner Cartridge Loaded</SingleInt>
	</Lookups>
</ValueLookup>
```

In our example, the lookup file has the following effect:

Value as Reported from HP Printer	Text Shown in PRTG (Channel)	Sensor Status Shown in PRTG	
0	Toner Okay	✅	Up

Value as Reported from HP Printer	Text Shown in PRTG (Channel)	Sensor Status Shown in PRTG	
1	Toner Low		Warning
2	No Toner Cartridge Loaded		Down

Customizing Lookups

To upload customized lookups to PRTG Hosted Monitor, see section Manage a PRTG Hosted Monitor Subscription.

If you want to change the status definitions of a channel, follow these steps:

1. Find out the (file) name of the default lookup file in the settings of the channel that you want to change the status definitions for.
2. From the \lookups subfolder of the PRTG program directory, copy this file into the \lookups\custom subfolder. Make sure that you do not change the file name.
   OR
   create a new .ovl file there.
   If you use the same ID in the ValueLookup tag, the files in the \lookups\custom subfolder have a higher priority than the original files in the \lookups folder. This way, PRTG prefers your customizations to the original lookup settings. If you want to use custom lookup definitions in addition to the standard lookups, define a new ID in the lookup file that is not used by any other lookup file. PRTG identifies lookup definitions via this ID, it does not use the file name.
3. Open the file with an XML or text editor and customize the lookups as you like. You can define your own text messages or customize sensor states for specific return values. For example, if you do not want a sensor to show the Down status for the return value 2 but only the Warning status, replace the state Error with Warning.

All possible states are specified in the LookupState.xsd file in the custom directory. Follow the schema of the .xml files that are delivered with PRTG to ensure that you safely edit lookups.

If you import an .oidlib file that contains lookups (you can see this in section Lookup in MIB Importer), you can define your own sensor states for the returned values. If you add an SNMP Library sensor and use this .oidlib file, PRTG creates a lookup definition file that uses the lookupname of the chosen library as id parameter. Override this lookup definition with your own custom lookup as described in this section. This is important because lookups that you add via an .oidlib file do not contain any status definitions and result in the Warning status of the sensor by default because of the entry undefinedState="Warning".

If you use an SNMP Custom String Lookup sensor, you can create a new custom lookup definition in the \lookups\custom subfolder with the expected return values. In this case, use the lookupname of the chosen library as id parameter to override the lookups from the .oidlib file.

When you save an edited lookup, make sure that you save it as an .ovl file. Otherwise, the lookup might accidentally be saved as a .txt file and might not be loaded.

Example for Lookups Customization

For example (for illustration purposes only), imagine you want

- the sensor to show the Warning status for all undefined values that the target device might return,
- to change the shown status for the return value 2 from the Down to the Warning status, and
- to add the state None (shown as the Unknown status) to the example above.

Then take the following steps:

1. Copy the file oid.paessler.hplaserjet.tonerstatus to the \lookups\custom subfolder of the PRTG program directory.
2. Open this file with a text editor.
3. Leave the id value unchanged to prioritize the customized lookup file.
4. Insert the status definition for undefined values into the ValueLookup element: undefinedState="Warning"
5. Replace the state Error with Warning for value 2.
6. Add a SingleInt element with the state None for the (hypothetical) return value 3.
7. Save the file and reload the custom lookup folder in PRTG.

The customized lookup file looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<ValueLookup id="oid.paessler.hplaserjet.tonerstatus" desiredValue="1"
undefinedState="Warning" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="PaeValueLookup.xsd">
	<Lookups>
		<SingleInt state="Ok" value="0">Toner Okay</SingleInt>
		<SingleInt state="Warning" value="1">Toner Low</SingleInt>
		<SingleInt state="Warning" value="2">No Toner Cartridge
Loaded</SingleInt>
		<SingleInt state="None" value="3">Unknown Status of Toner</SingleInt>
	</Lookups>
</ValueLookup>
```

See also the SNMP Custom String Lookup sensor for a lookup definition that maps a string value to a sensor status.

desiredValue Attribute

It is necessary to define a desiredValue in the lookup files. The desiredValue corresponds to a status value that triggers a lookup. PRTG calculates the percentage of time this specific status was monitored. PRTG displays the result for all data tables and graphs that show averaged values.

Considering the example above where the desiredValue is 1, PRTG calculates the percentage of time that the toner status showed the Warning status. If, during a time span of five minutes, four of five sensor scans returned Warning, PRTG shows an average of 80% for this time span because 80% of the time, the sensor showed the Warning status.

The desiredValue attribute always has to be an integer. For the lookup type Range, use an integer that you defined for one of your "from" or "to" parameters in the lookup file.

For more information, see also the Knowledge Base: Can I graph text values?

Lookup Types: SingleInt, Boolean, BitField, Range

Besides the lookup type SingleInt as seen above, there are three other lookup types: Boolean, BitField, and Range. Using these types, you can define lookup values beyond simple integers.

Lookup Type	Description	Syntax
SingleInt	Use an integer to define a lookup for one status value.	value="int" PRTG supports the full 32-bit integer range.
Boolean	Use 0 or 1 to define a lookup for two different status values.	value="0" value="1"
BitField	Use a bitfield for multiple status values.	Only use this lookup type if you have some basic knowledge of bitmasks. See section More 3614 for a general introduction. Every value has to be zero (0) or has to equal a power of two (for example, 1, 2, 4, 8, 16, 32, 64, etc.). The SNMP Custom String Lookup sensor does not support BitFields.
Range	Use an inter range from-to to define a lookup for several status values.	from="int" to="int" Using ranges, the parameters "from" and "to" must always be defined. If you want to query only one single value in a range file, this value must be set as a parameter for "from" and "to" (for example, from="2" to="2"). See also the Knowledge Base: Custom lookup range. The SNMP Custom String Lookup sensor does not support ranges. The full 32-bit integer range is supported.

You can use only one kind of lookup type in one lookup file. This means, only SingleInt, only Boolean, only BitField, or only Range. Different lookup types in one file are not allowed.

Define Lookup Files in Channel Settings

For each sensor with a custom channel, you can define a lookup file to use with the option Lookup in the channel settings. This option is visible for many SNMP sensors, some application sensors, and always for the following sensors:

- EXE/Script
- EXE/Script Advanced (if you define a Custom unit)
- SNMP Custom

For details, see section Channel Settings 3121.

Loading Lookups

You can (re)load the lookups in the custom folder by going to Setup | System Administration | Administrative Tools 3352 in the PRTG web interface and clicking Go! under Load Lookups and File Lists.

A sensor whose lookup file you have modified and reloaded does not re-evaluate this lookup before the next sensor scan. For sensors with long scanning intervals, use the Scan Now option from the context menu 240 to immediately apply the new lookup definition and to avoid an incorrect sensor status.

Debugging

What happens if...

- a return value is defined in the lookups that is never returned by a device because the value is not assigned? The value is never triggered, so PRTG ignores this entry.
- PRTG receives a return value that is not defined for lookups? No substitution message can be found. PRTG only shows the return value. You can optionally define a status for unknown values with a definition of undefinedState in the ValueLookup element (see section The XML Schema 3608).
- different lookup types are in one lookup file? This is not allowed and PRTG discards this lookup definition. If you use miscellaneous lookup types in one file, for example, ranges and SingleInts together, PRTG creates a ticket when loading lookups or restarting the PRTG core server with the following error message: Lookup file "[...]" could not be loaded ("" is not a valid integer).
- XML code is incorrect? PRTG creates a new ticket when it loads lookups or restarts the PRTG core server with a corresponding error message and discards this lookup definition.
- a lookup file has a file extension other than .ovl? The file is not loaded.
- alerting is disabled or based on limits? Error and Warning states that are defined in the lookup do not apply. Make sure that you select the option Enable alerting based on lookups in the channel settings if you want to use lookup definitions to control the sensor status.
- you define a scaling factor in channel settings? This does not modify the values that are defined by lookups. Any applied lookup always uses the raw value as retrieved from the target device. If you use a scaling factor for such a channel, you notice the scaling in data graphs but the channel value appears unmodified in data tables.

More

KNOWLEDGE BASE

Custom lookup range

- https://kb.paessler.com/en/topic/55493

Can I graph text values?

- https://kb.paessler.com/en/topic/73062

VIDEO TUTORIAL

How to configure lookups in PRTG

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

PAESSLER TOOLS

MIB Importer

- https://www.paessler.com/tools/mibimporter

14.7 Regular Expressions

For some sensors, you can use regular expressions (regex) to match a search pattern. PRTG supports Perl Compatible Regular Expression (PCRE).

The following sensors support regex:

- DHCP
- File Content
- HTTP Advanced
- IMAP
- Port
- SNMP Custom String
- WMI Custom String

You can only use regex for the respective sensors if you explicitly enable regex in the sensors' settings.

PRTG supports regex options in the form (?isgmxUJ) and their negations, for example, (?-i). PRTG does not support regex flags like /g (global), /s (single line), or /gs, and does not correctly search for the target string if you try to set flags.

Common Search Patterns

Find matches that contain the word error or alarm:

```
\b(error|alarm)\b
```

Find matches that contain the word ERROR, not error, using case sensitivity:

```
(?-i)\bERROR\b
```

Find matches that contain the words error and alarm, in any order:

```
(?=.*\berror\b)(?=.*\balarm\b).*
```

Find matches that contain all of the words tree, flower, leaf, and bug, in any order:

```
(?=.*\btree\b)(?=.*\bflower\b)(?=.*\bleaf\b)(?=.*\bbug\b).*
```

It is not possible to match an empty string with the regex search with sensors.

Example

The search pattern

```
(?i)(?=.*\berror\b)(?=.*\balarm\b).*
```

matches the following expressions:

- Alarm error
- Error alarm

- I am an error and I trigger an alarm.
- I am an alarm and I indicate an error.
- An alarm combined with an error indeed!
- An error combined with an alarm, too!

14.8 Calculating Percentiles

PRTG not only monitors your network and informs you in the case of issues that are worth a closer look, it also stores a lot of historic data that it gathers from your sensors. This means that you have a base for the statistical analysis and evaluation of what is and was happening in your network. When you create a report 3192 or a historic data report 183, you get raw data, sums, averages, and percentages of your monitoring data.

Additionally, PRTG also offers percentile calculation. This statistical method arranges your data, for example, from the lowest value to the highest value, and calculates the percentile that you want, optimally informing you about the distribution of your network-relevant data.

ⓘ For example, if you request the 95th percentile, you know that 95 percent of the measured data is below a certain value and PRTG can tell you what this certain value is.

If applied to bandwidth, for example, you know which values you have when talking about the 5 percent of unusually high bandwidth consumption, and which value your users do not exceed 95 percent of the time. Service providers often use percentiles to offer billing that excludes infrequent usage peaks.

If you want to know more about the formula that PRTG uses for percentile calculation, see the Knowledge Base: What are percentiles and what differences do they make in PRTG reports?

More

KNOWLEDGE BASE

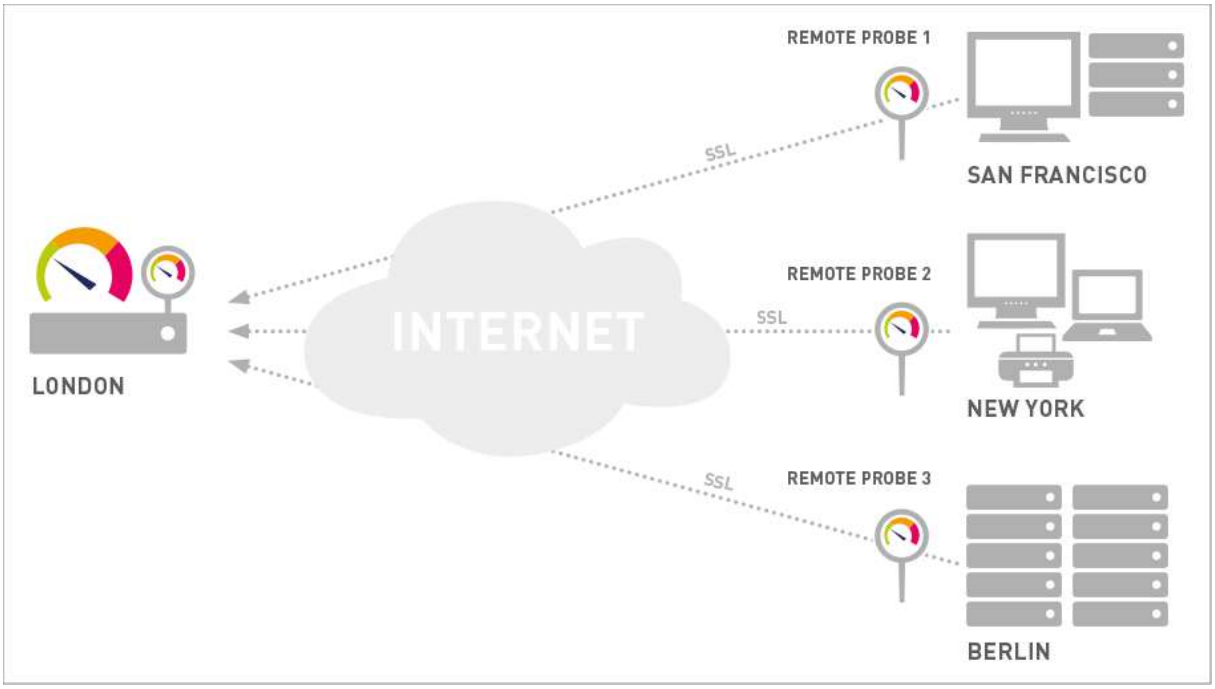
What are percentiles and what differences do they make in PRTG reports?

- https://kb.paessler.com/en/topic/9563

14.9 Add 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.



Monitoring Remote Locations via Remote Probes

For instructions on how to add a remote probe, see the following sections:

- Background information: Remote Probes and Multiple Probes 3621
- Step-by-step installation: Install a Remote Probe 106
- Partially automatic installation: Remote Probe Setup via Device Tools 3625
- Quick installation guide on the Paessler website: How to install a PRTG remote probe in 4 steps

More

PAESSLER WEBSITE

How to install a PRTG remote probe in 4 steps

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

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

14.9.1 Remote Probes and Multiple Probes

Upon installation, PRTG automatically creates the first probe, namely the local probe in PRTG Network Monitor, and the hosted probe in PRTG Hosted Monitor. They run on the PRTG core server system and monitor all reachable devices, servers, and services from the system, using the sensors you configure.

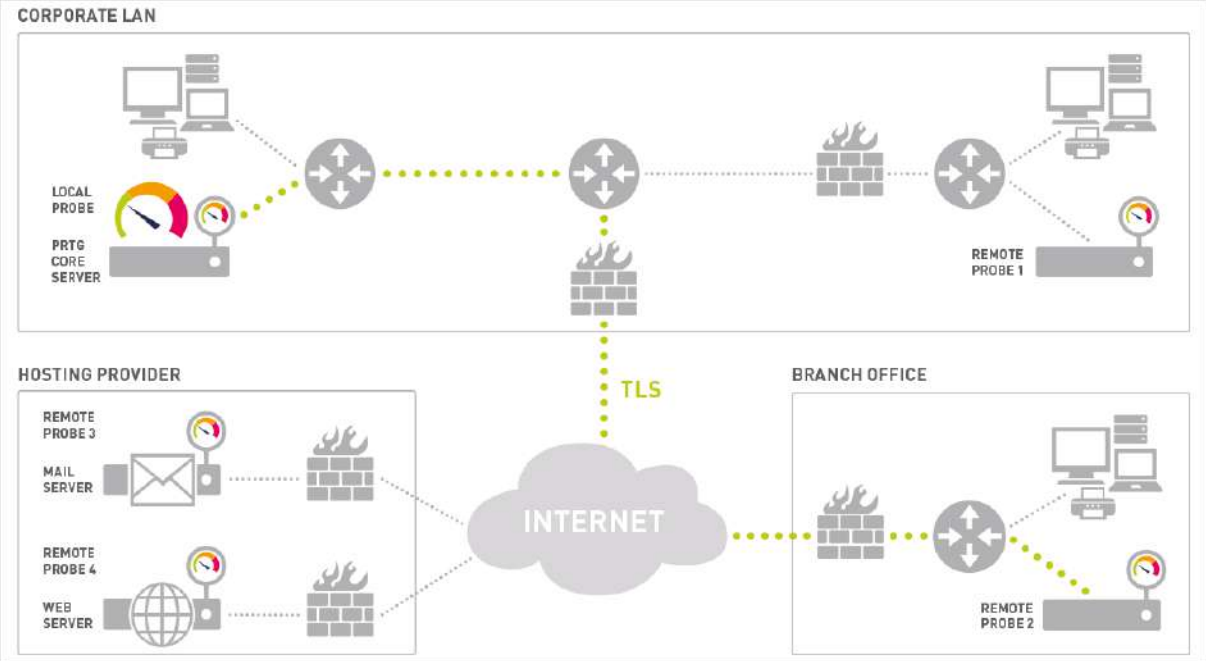
Working only with a local probe should suffice for LAN monitoring with PRTG Network Monitor and if you want to monitor one location only. For LAN monitoring with PRTG Hosted Monitor, at least one remote probe is required because the hosted probe can only reach targets that are publicly available via the internet.

Scenarios That Require Remote Probes

There are several situations that make it necessary to work with remote probes in the same LAN or in remote locations. Among these situations are the following:

- You use PRTG Hosted Monitor and want to monitor your local network.
- You have more than one location and you need to make sure that services are available from all locations.
- Your network is divided into several LANs that are separated by firewalls, and the local probe cannot monitor specific services across these firewalls.
- You want to monitor systems in a secure network and you need a secure connection between the PRTG core server and that network.
- You want to sniff packets on a different computer.
- You want to monitor NetFlow data on a different computer.
- You experience performance issues with CPU-intensive sensors like Packet Sniffer or NetFlow sensors and need to distribute the load among more than one computer.

The following chart shows an example for a remote probe scenario.



Monitoring a Distributed Network with PRTG

The PRTG core server inside the corporate LAN (top left) can monitor:

- Services that are inside the corporate LAN using the local probe.
- Services that are behind a firewall in the corporate LAN using remote probe 1.
- Secured services that are inside the branch office (bottom right) using remote probe 2.
- Secured services on mail server and web server using remote probe 3 and remote probe 4 installed directly on these servers.
- Public services on the internet using any of the probes.

How Probes Work

As soon as a probe starts, it automatically connects to the PRTG core server 125, downloads the sensor configuration, and begins its monitoring tasks. The PRTG core server sends new configuration data to a probe as soon as the user changes the monitoring configuration. Probes monitor autonomously and send the monitoring results back to the PRTG core server for each check that they perform.

If the connections between the PRTG core server and a probe fail for any reason (for example, restarting the PRTG core server system), the probe continues to monitor and stores the results. During a connection loss, a buffer stores a maximum of 500,000 sensor results in the RAM of the remote probe system (up to 50 - 200 MB). This means that for 100 sensors with a 1-minute scanning interval, the probe can buffer the monitoring results of up to 3 days (or 52 minutes for 10,000 sensors with a 1-minute scanning interval). The probe automatically reconnects to the PRTG core server as soon as it is available again and transmits all monitoring results that it gathered during the connection loss.

The connection between a probe and the PRTG core server is initiated by the probe and is secured with Secure Sockets Layer (SSL)/Transport Layer Security (TLS). This means that the data that is sent back and forth between the PRTG core server and the probe is not visible to someone that is capturing data packets. The PRTG core server provides an open TCP/IP port and waits for connection attempts from probes. If a new probe connects for the first time, you receive a ToDo ticket 211 and then you see the new probe in the device tree.

As a security precaution, you must manually approve the probe in the device tree before you can create any sensors. You can also deny a probe. PRTG then disconnects it. PRTG accepts no further connection attempts and it adds the probe IP address to the Deny IP Addresses list in the probe's system settings 3325. This ensures that unauthorized probes cannot connect to a PRTG core server.

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 run PRTG in a cluster, remote probes also connect to all cluster nodes and send monitoring data. This works as described above for a single PRTG core server. If the master node fails, you can still see monitoring data on the failover nodes. You can define the Cluster Connectivity of each probe in the probe's settings 515, section Administrative Probe Settings.

Automatic Probe Update

Whenever you install a new version of PRTG on the PRTG core server, all remote probes automatically download and install the updated version as soon as they reconnect to the updated PRTG core server.

PRTG updates the local probe when you update the PRTG core server. All remote probes automatically download the new binaries via the SSL/TLS-secured probe connection or PRTG core server connection. Downloading the 4-MB file takes anywhere from a few seconds (in LANs) up to a few minutes (via internet connections), depending on the available bandwidth. As soon as the update is downloaded, the remote probe disconnects, installs the update, and reconnects to the PRTG core server. This takes between 20 and 100 seconds. Note that during the update phase, monitoring by the local probe can be affected because of the bandwidth that is required for the downloads.

ⓘ If a remote probe keeps disconnecting after an update, check if the server with the remote probe has two network connections with different IP addresses. Make sure that these addresses are in the list of allowed IP addresses in the Core & Probes 3327 settings.

Delete Remote Probe

If you delete a connected remote probe via the device tree, it stops the PRTG probe service on the remote probe system and sets the startup type to manual. We recommend that you additionally uninstall the remote probe on the remote probe system.

If you delete a disconnected remote probe, it does not stop the PRTG probe service on the remote probe system and does not affect the startup type. The remote probe will continue to try to reconnect to the PRTG core server until you manually stop the PRTG probe service or uninstall the remote probe on the remote probe system.

More

PAESSLER WEBSITE

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

14.9.2 Remote Probe Setup via Device Tools

You can directly install a remote probe via the context menu[234] of a device in the device tree. This partially automatic installation mechanism is an alternative to the Remote Probe Installer[106]. For a quick installation guide, see the Paessler website: How to install a PRTG remote probe in 4 steps.

This is an experimental feature. It might not work in all situations. In this case, see section Debugging[3629].

This feature is not available in PRTG Hosted Monitor.

You cannot install a remote probe on the local probe device or hosted probe device. The Remote Probe Setup via Device Tools is also not available for devices on remote probes. In this case, use the Remote Probe Installer.

If you run PRTG in a cluster, see Cluster and Remote Probes Outside the LAN[3627].

Steps to Take

To install a remote probe directly from the device tree in the PRTG web interface, follow these steps:

- Step 1: Meet the Requirements[3625]
- Step 2: Prepare the PRTG Core Server[3626]
- Step 3: Configure the Failover Node[3628]
- Step 4: Confirm the Failover Node[3628]
- Step 5: Approve the New Remote Probe[3629]

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?

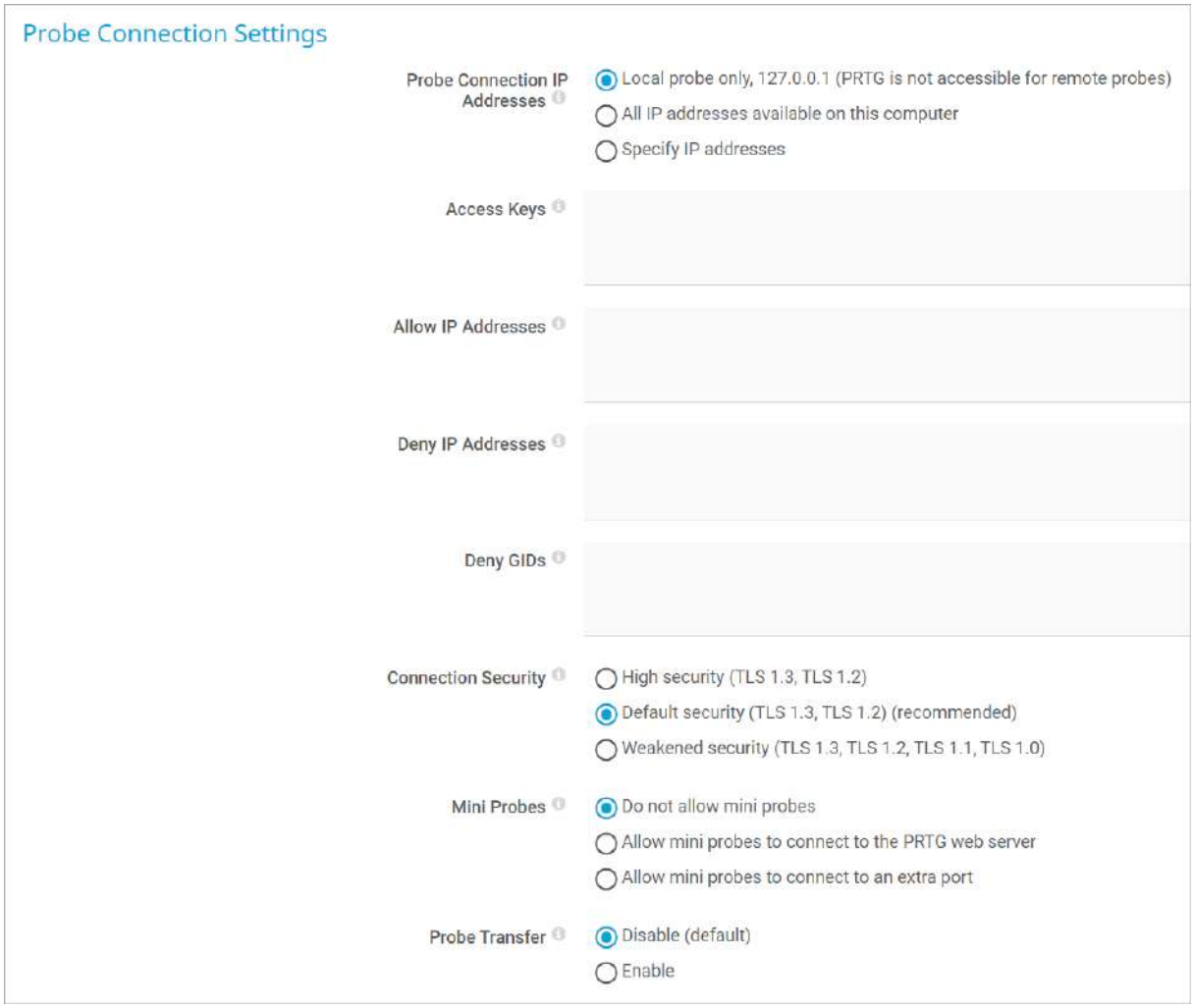
PRTG Network Monitor and PRTG Hosted Monitor already include a local probe or hosted probe on the PRTG core server. This is why you cannot additionally install a remote probe on your PRTG core server system.

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

Step 2: Prepare the PRTG Core Server

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: Configure the Failover Node

If you have not yet done so, add a device [365] that represents the target system on which you want to install the remote probe. Set the correct Windows credentials for this device.

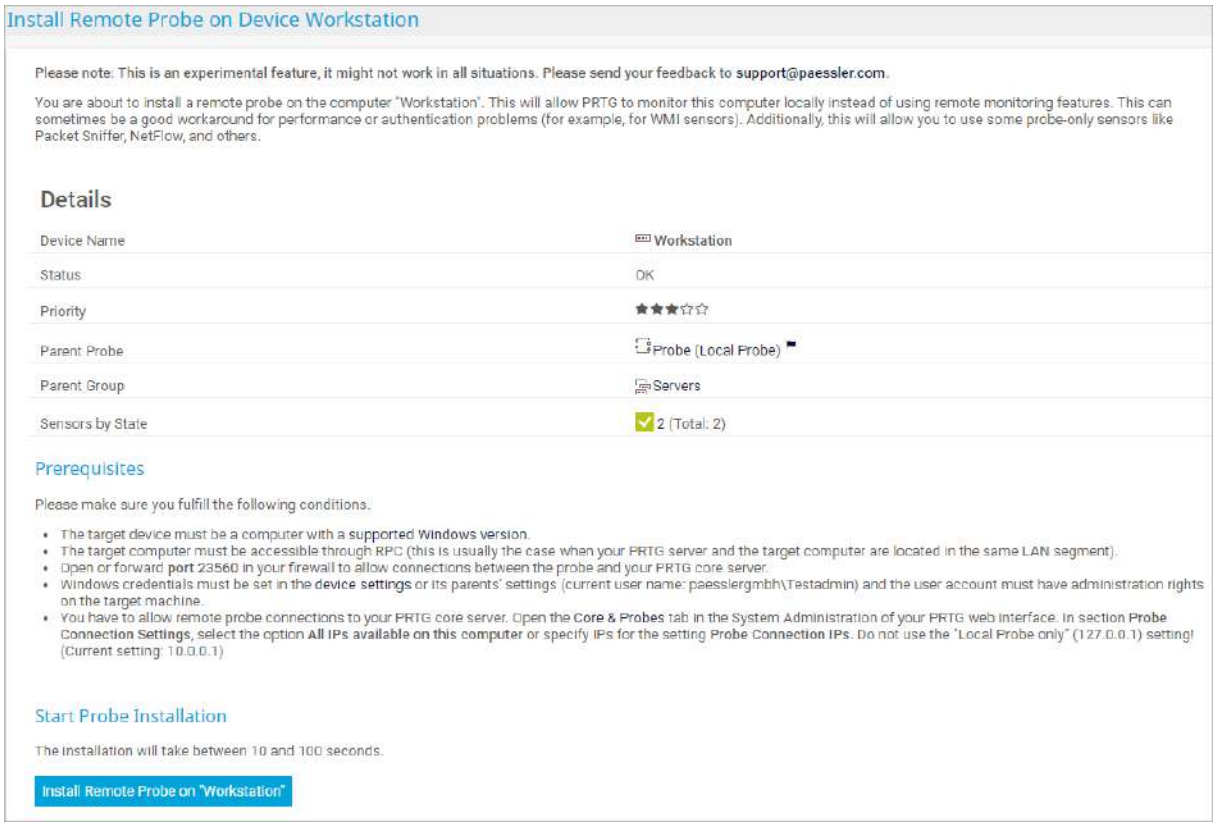
1. Open the device settings [588].
2. In the Credentials for Windows Systems section, provide Domain or Computer Name, User Name, and Password for the target system. You can also inherit [135] the credentials from the settings of a parent object in the device tree.

ⓘ Make sure that this user account has administration rights on the target system.

Step 4: Confirm the Failover Node

1. In the device tree, open the context menu [234] of the target device.
2. Select Device Tools | Install Remote Probe to open the install dialog in a new window.

ⓘ This option is only available for devices on the local probe of PRTG Network Monitor.

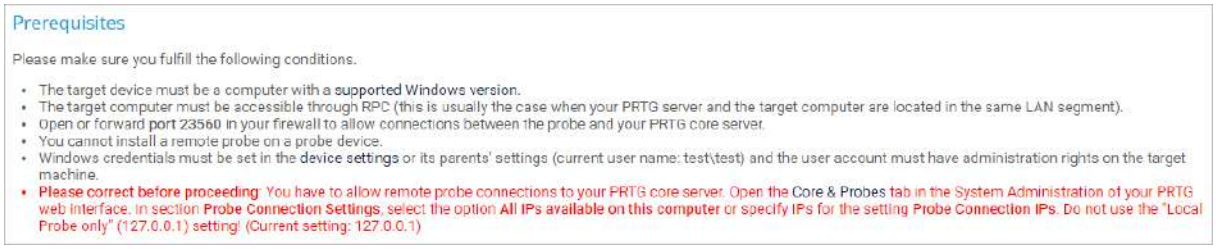


Remote Probe Installation Dialog

The install dialog includes four sections:

- Experimental feature notice and short introduction
- Details: Overview of the device like Device Name, Status, Priority, Parent Probe, Parent Group, and Sensors by State.

- Prerequisites: Make sure that you meet the requirements listed here. If not, PRTG cannot start the installation process. Open requirements are highlighted in red.



Installation Unable to Start Because Prerequisites Are Not Met

- Start Probe Installation: Time estimation for the installation and installation start button

If all prerequisites are met, you can install the remote probe on the target system by clicking Install Remote Probe on "[device name]". Wait until the process has ended. If the installation is successful, the following message appears in the Start Probe Installation section: Done. Result is: OK.

ⓘ Every time you start an installation, PRTG automatically adds a new key to the field Access Keys in the Core & Probes 3325 settings, no matter if the installation is successful or not.

Step 5: Approve the New Remote Probe

If the installation is successful, you receive further instructions after the result message. You also receive a new ToDo ticket 211.

Click Approve and auto-discover to acknowledge the new remote probe and to instantly start an auto-discovery 264 in this network. Click Approve new probe to acknowledge the new remote probe without running an auto-discovery. You can also discard the remote probe by clicking Deny.

ⓘ When you deny or remove a remote probe, this device's global ID (GID) is listed in the Deny GIDs field in the Core & Probes 3325 settings. Future probe connections from this device are automatically denied.

ⓘ When you deny the remote probe in the device tree, this 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.

Wait while the remote probe connects. Once the remote probe has connected, you can create groups, devices, and sensors to customize your monitoring via the new remote probe.

Debugging

- Note that installing a remote probe directly from the device tree in the PRTG web interface is an experimental feature. This approach might not be possible in all situations.
- Make sure you meet all the requirements as described in step 1 3625 such as the Windows Firewall settings.
- If the quick installation procedure as described in this section does not work with your setup, manually install the remote probe via the Remote Probe Installer as described in section Install a Remote Probe 106.

More

KNOWLEDGE BASE

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

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

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

14.10 Failover Cluster Configuration

A failover cluster consists of two or more PRTG core servers that work together to form a high availability monitoring system. PRTG offers the single failover cluster (one master node and one failover node) in all licenses, including the Freeware Edition.

This feature is not available in PRTG Hosted Monitor.

Illustration of a Single Failover Cluster

For more information about clusters in general, see section Failover Cluster 128.

Before You Start

Consider the following notes about clusters.

- You need two target systems that run any Windows version (as of Windows 7). The target systems can be physical machines or virtual machines (VM). For more information, see section System Requirements 23.
- The machines must be up and running.
- The machines must be similar in regard to the system performance and speed (like CPU, RAM, etc.).
- In a cluster, each of the cluster nodes individually monitors the devices that you add to the cluster probe. This means that the monitoring load increases with every cluster node. Make sure that your devices and your network can handle these additional requests. Often, a longer scanning interval for your entire monitoring setup is a good idea. For example, set a scanning interval of five minutes in the root group's settings 419.
- We recommend that you install PRTG on dedicated, physical machines for best performance.
- Keep in mind that a machine that runs a cluster node might automatically restart without prior notice, for example, because of special software updates.
- Both machines must be visible for each other through the network.
- Communication between the two machines must be possible in both directions. Make sure that no software or hardware firewall blocks communication. All communication between cluster nodes is directed through one specific Transmission Control Protocol (TCP) port. You define the port during the cluster setup. By default, it is TCP port 23570.

- In a cluster, a Domain Name System (DNS) name that you enter under Setup | System Administration | User Interface in the PRTG web interface is only used in links that point to the master node. You cannot enter a DNS name for a failover node. This means that any HTTP or HTTPS links that point to a failover node (for example, in notifications or in maps) always point to the failover node's IP address in your local network and might therefore not be reachable from external networks or from the internet, particularly if you use network address translation (NAT) rules.
- Email notifications for failover: The failover master node sends notifications if the primary master node is not connected to the cluster. To ensure that PRTG can deliver emails in this case, configure the notification delivery 3315 settings so that PRTG can use them to deliver emails from your failover node as well. For example, use the option to set up a secondary Simple Mail Transfer Protocol (SMTP) email server. This fallback server must be available for the failover master node so that it can send emails over it independently from the first email server.
- Make your machines secure. Every cluster node has full access to all stored credentials, other configuration data, and the monitoring results of the cluster. Also, PRTG software updates can be deployed from every cluster node. So, make sure you take security precautions to avoid security attacks like hackers and Trojans. Secure every cluster node as carefully as the master node.
- Run cluster nodes either on 32-bit or 64-bit Windows versions only. Avoid using both 32-bit and 64-bit versions in the same cluster. This configuration is not supported and might result in an unstable system. Also, ZIP compression for the cluster communication is disabled and you might encounter higher network traffic between your cluster nodes.
- If you run cluster nodes on Windows systems with different time zone settings and you use schedules 3284 to pause monitoring of sensors, the schedules apply at the local time of each cluster node. Because of this, the overall status of a particular sensor is shown as Paused every time the schedule matches a cluster node's local system time. Use the same time zone setting on each Windows system with a cluster node to avoid this behavior.
- The password for the PRTG System Administrator user account is not automatically synchronized on cluster nodes. The default credentials (prtgadmin) for the PRTG System Administrator user account do not work on the failover node. For more information, see the Knowledge Base: I cannot log in to my failover node anymore. What can I do?
- Stay below 2,500 sensors per cluster for best performance in a single failover. Clusters with more than 5,000 sensors are not officially supported. For each additional failover node, divide the number of sensors by two.

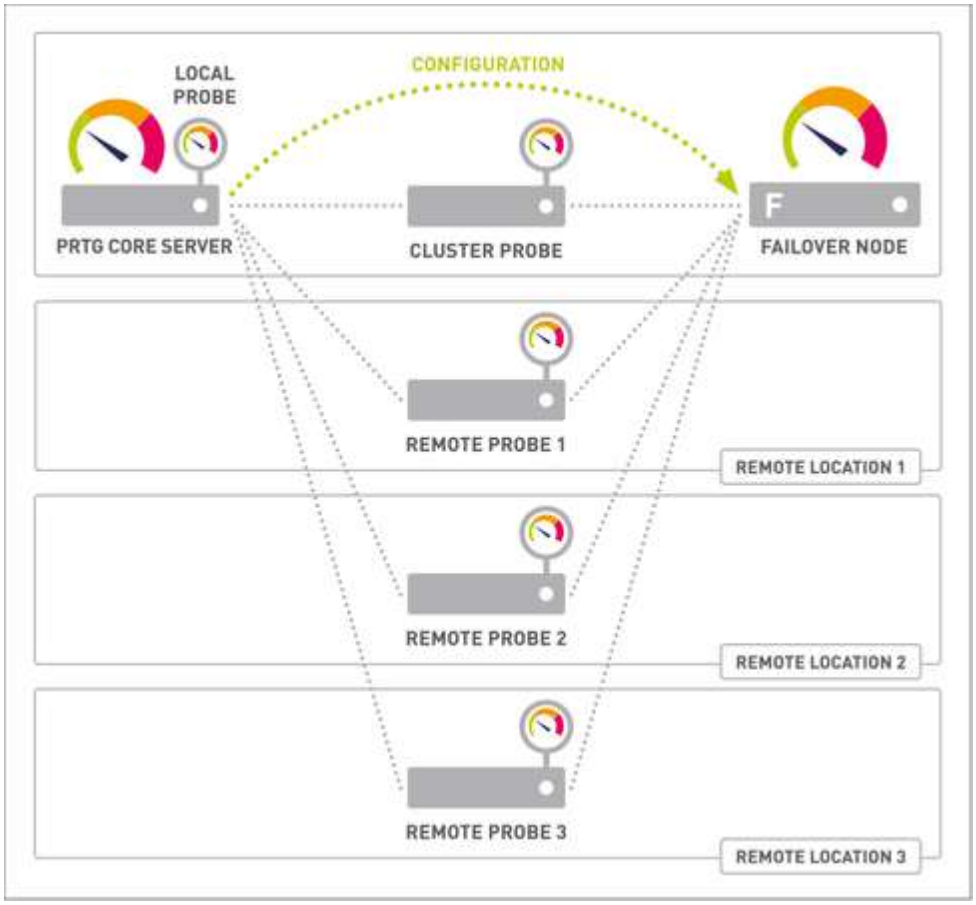
In cluster mode, you cannot use sensors that wait for data to be received. Because of this, you can use the following sensors only on a local probe or remote probe 125:

- DHCP
- HTTP Push Count
- HTTP Push Data
- HTTP Push Data Advanced
- IPFIX and IPFIX (Custom)
- jFlow v5 and jFlow v5 (Custom)
- NetFlow v5 and NetFlow v5 (Custom)
- NetFlow v9 and NetFlow v9 (Custom)
- Packet Sniffer and Packet Sniffer (Custom)
- sFlow and sFlow (Custom)
- SNMP Trap Receiver

- Syslog Receiver

Remote Probes in a Cluster

PRTG provides cluster support for remote probes. This means that all of your remote probes can connect to all of your cluster nodes. Because of this, you can still see the monitoring data of remote probes and sensor warnings and errors even when your master node fails.



Remote Probes with Cluster Connectivity

Consider the following notes about clusters with remote probes:

- You must allow remote probe connections to your failover nodes. To do so, log in to each system in your cluster and open the PRTG Administration Tool 3473. On the PRTG Core Server tab, accept connections from remote probes on each cluster node.
- If you use remote probes outside your local network: You must use IP addresses or Domain Name System (DNS) names for your cluster nodes that are valid for both the cluster nodes to reach each other and for remote probes to reach all cluster nodes individually. Open the Cluster 3356 settings and adjust the entries for cluster nodes accordingly so that these addresses are reachable from the outside. New remote probes try to connect to these addresses but cannot reach cluster nodes that use private addresses.
- If you use network address translation (NAT) with remote probes outside the NAT: You must use IP addresses or DNS names for your cluster nodes that are reachable from the outside. If your cluster nodes are inside the NAT and the cluster configuration only contains internal addresses, your remote probes from outside the NAT are not able to connect. The PRTG core server must be reachable under the same address for both other cluster nodes and remote probes.

- A remote probe only connects to the PRTG core server with the defined IP address when it starts.
  ⓘ This PRTG core server must be the primary master node.
- Initially, remote probes are not visible on failover nodes. You need to set their Cluster Connectivity first in the Administrative Probe Settings 515 for them to be visible and to work with all cluster nodes. Select Remote probe sends data to all cluster nodes for each remote probe that you want to connect to all cluster nodes.
- Newly connected remote probes are visible and work with all cluster nodes immediately after you acknowledge the probe connection. The connectivity setting Remote probe sends data to all cluster nodes is default for new remote probes.
- As soon as you activate a remote probe for all cluster nodes, it automatically connects to the correct IP addresses and ports of all cluster nodes.
- Once a remote probe has connection data from the primary master node, it can connect to all other cluster nodes also when the primary master node fails.
- Changes that you make in the connection settings of cluster nodes are automatically sent to the remote probes.
- If a PRTG core server (cluster node) in your cluster is not running, the remote probes deliver monitoring data 3622 after the PRTG core server restarts. This happens individually for each PRTG core server in your cluster.
- If you enable cluster connectivity for a remote probe, it does not deliver monitoring data from the past when cluster connectivity was disabled. For sensors that use difference values, the difference between the current value and the last value is shown with the first new measurement (if the respective sensor previously sent values to the PRTG core server).
- Except for this special case, all PRTG core servers show the same values for sensors on devices that you add to the cluster probe.
- The PRTG core server that is responsible for the configuration and management of a remote probe is always the current master node. This means that only the current master node performs all tasks of the PRTG core server. If you use a split cluster with several master nodes, only the master node that appears first in the cluster configuration is responsible.

ⓘ You can use remote probes in a cluster as described above, which is showing monitoring data of all remote probes on all cluster nodes. However, you cannot cluster a remote probe itself. To ensure gapless monitoring for a specific remote probe, install a second remote probe on a machine in your network next to the remote probe. Then create all devices and sensors of the original remote probe on the second remote probe by cloning 3154 the devices from the original remote probe, for example. The second remote probe is then a copy of the first remote probe and you can still monitor the desired devices if the original remote probe fails.

ⓘ Remote probes that send data to all cluster nodes result in increased bandwidth usage. Select Remote probe sends data only to primary master node in the probe settings 515 for one or more remote probes to lower bandwidth usage if necessary.

ⓘ Explicitly check on each cluster node if a remote probe is connected. PRTG does not notify you if a remote probe is disconnected from a cluster node. For example, log in to the PRTG web interface on a cluster node and check in the device tree if your remote probes are connected.

More

KNOWLEDGE BASE

What is the clustering feature in PRTG?

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

What are the bandwidth requirements for running a cluster?

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

What is a failover master node and how does it behave?

- https://kb.paessler.com/en/topic/7663

I need help with my cluster configuration. Where do I find step-by-step instructions?

- https://kb.paessler.com/en/topic/41913

Cluster: How do I convert a (temporary) failover master node to be the primary master node?

- https://kb.paessler.com/en/topic/34853

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

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

I cannot log in to my failover node anymore. What can I do?

- https://kb.paessler.com/en/topic/89878

PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

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

How to set up a failover cluster in PRTG in 6 steps

- https://www.paessler.com/support/how-to/failover-cluster

14.11 Data Storage

PRTG stores the monitoring configuration, monitoring data, logs, tickets, and reports, as well as support and debug data into different subfolders in the PRTG data directory on the probe system. Additionally, there is data in the PRTG program directory (for example, scripts for your custom sensors[3116]) and in the Windows registry.

You cannot access these directories in PRTG Hosted Monitor.

In this section:

PRTG Program Directory

32-bit systems:

```
%programfiles%\PRTG Network Monitor
```

64-bit systems:

```
%programfiles(x86)%\PRTG Network Monitor
```

These are the default paths. If you specified a different installation directory, you find your data there.

Subfolders in the PRTG Program Directory

The following folder is stored in the PRTG data directory:

Folder	Description	File Format
\Support Bundle	Collected and compressed log file data when sending a support bundle to the Paessler support team For more information, see the Knowledge Base: What is the best way to contact the Paessler support team?	LOG / TXT / ZIP

PRTG Data Directory

On supported Windows versions:

```
%programdata%\Paessler\PRTG Network Monitor
```

ⓘ These are the default paths, depending on your Windows version. If you specified a custom path for data storage, you need to look it up in the PRTG Administration Tool 3473 on the PRTG Core Server tab. You find the path there.

ⓘ The Windows ProgramData folder is hidden by default. To display it, you need to enable hidden items in the View options of your Windows system.

ⓘ You can find the supported Windows versions in section System Requirements 27.

Files and Subfolders in the PRTG Data Directory

The following files are stored in the PRTG data directory:

File	Description	File Format
PRTG Configuration.dat	Monitoring configuration (for example probes, groups, devices, sensors, users, maps, reports, and more)	Extensible Markup Language (XML)
PRTG Configuration.old	Backup of previous version of monitoring configuration	XML
PRTG Graph Data Cache.dat	Precalculated data for the graphs throughout the PRTG web interface (if missing, this file is automatically recalculated from the files in the monitoring database)	Proprietary

The following folders are stored in the PRTG data directory:

Folder	Description	File Format
\Configuration Auto-Backups	Backup versions of the file PRTG Configuration.dat	ZIP / XML
\Log Database	Database with the recent event history for the whole system: menu option Logs in the PRTG web interface	Raw data format (DB)
\debug	Text file based logs of the PRTG core server system and the probe system	TXT

Folder	Description	File Format
\sensors	Text file based debug logs of the sensors (files named after the ID of a sensor; logs are written only if activated in a sensor's settings)	TXT
\core	Text file based logs of the PRTG core server system, the probe system, the cluster system, and result files for certain sensors	TXT
\webserver	HTTP server log files of the PRTG web server	Standard web server log format
\Monitoring Database	Results of all monitoring requests for all sensors (required for historic reports)	Proprietary
\Report PDFs	Older PDF reports 3192 stored in the file system	PDF
\reporter	Screenshots created for reporting issues to the Paessler support team	PNG
\Screenshots (Fullpage Sensor)	Screenshots stored by the PhantomJS browser engine of the HTTP Full Web Page sensor	JPG (in subfolders)
\StreamLog	Data log files for Packet Sniffer and Flow (NetFlow, jFlow, sFlow, IPFIX) sensors (only available if activated in the sensor settings)	
\Syslog Database	Received Syslog messages	Proprietary
\System Information Database	Retrieved system information 202 for the categories hardware, users (loggedonusers), processes, services, software, system (in according subfolders)	Proprietary (in JavaScript Object Notation (JSON) format)
\ToDo Database	Database with all ToDo entries	Raw data format (DB) ⓘ Deprecated as of PRTG 14.1.8
\Ticket Database	Database with all tickets 211 (ticketdata.dat)	Raw data format (DAT)
\Toplist Database	Database for historic Toplists for Packet Sniffer and flow sensors	Raw data format (TOP)

Folder	Description	File Format
\Trap Database	Received SNMP Trap messages	Proprietary

Structure of the Logs Folder

Folder	Description	File Format
\appserver	Currently not in use	N/A
\core	Text file based logs of the PRTG core server system and the cluster system	TXT
\debug	Text file based debug logs of the PRTG core server system and probe system, and PRTG core server cache recalculation	TXT
\desktopclient	Currently not in use	N/A
\enterpriseconsole	Text file based logs of the deprecated Enterprise Console	TXT
\probe	Text file based logs of the probe system	TXT
\reporter	Text file based logs of creating PDF reports and screenshots for the Paessler support team	TXT
\sensordeprecation	Text file based log of deprecated sensors	TXT
\sensors	Text file based logs of sensors	TXT
\serveradmin	Text file based logs of the administration system	TXT
\webserver	HTTP server log files of the PRTG web server	TXT

Windows Registry

System settings on 32-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Paessler\PRTG Network Monitor
```

System settings on 64-bit systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Paessler\PRTG Network Monitor
```

HTTP Full Web Page Sensor: Cached Files

If you use the HTTP Full Web Page, files might be cached in this directory:

```
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
```

Auto-Update Files

PRTG automatically saves downloaded software versions in the \download subfolder of the PRTG program directory. The compressed prtg.zip file that contains all necessary files is also cached there.

More

KNOWLEDGE BASE

What is the best way to contact the Paessler support team?

- https://kb.paessler.com/en/topic/57993

Part 15
Appendix

15 Appendix

Find further information about PRTG and used terms in the following sections.

15.1 Differences between PRTG Network Monitor and PRTG Hosted Monitor

See below for the differences between the settings and features that PRTG Network Monitor and PRTG Hosted Monitor have to offer.

Licensing, Payment, Infrastructure

Topic	PRTG Network Monitor	PRTG Hosted Monitor
Trial period	30 days	10 days
Freeware Edition	Freeware (100 sensors) available	No freeware available, smallest edition is Hosted 500
Payment	One-time license fee plus annual maintenance	Monthly or annual subscription
Change of subscription or license size	License: up only	Subscription: up and down, anytime
Maximum installation size	Max. 10,000 sensors recommended	10,000 sensors
PRTG update management	Done by user	Done by Paessler

Features

Feature	PRTG Network Monitor	PRTG Hosted Monitor
Local probe	Yes	No
Hosted probe	No	Yes
Cluster	Yes	No
Freeware Edition (100 sensors)	Yes	No
Remote Desktop Protocol (RDP) access to PRTG core server	Yes	No

Feature	PRTG Network Monitor	PRTG Hosted Monitor
Historic data purging (manually defined)	Yes	No
Active Directory integration	Yes	No
License/subscription settings via PRTG web interface	Yes	No
Recommended sensors on local probe/hosted probe	Yes	No
Auto-discovery for groups on local probe/hosted probe	Yes	No
Mini probes	Yes	No
Device tools on local probe/hosted probe	Yes	No
Proxy server settings	Yes	No
System information on local probe/hosted probe	Yes	No
PRTG Administration Tool on PRTG core server	Yes	No
Notification methods:		
▪ Send Email	Yes	Yes
▪ Send SMS/Pager Message	Yes	Yes
▪ Execute HTTP Action	Yes	Yes
▪ Send Amazon Simple Notification Service Message	Yes	Yes
▪ Assign Ticket	Yes	Yes
▪ Send Push Notification	Yes	Yes

Feature	PRTG Network Monitor	PRTG Hosted Monitor
▪ Send Microsoft Teams Message	Yes	Yes
▪ Send Slack Message	Yes	Yes
▪ Send MQTT Publish Notification	Yes	Yes
▪ Send OPC UA Notification	Yes	Yes
▪ Add Entry to Event Log	Yes	No
▪ Send Syslog Message	Yes	No
▪ Send SNMP Trap	Yes	No
▪ Execute Program	Yes	No
Re-login request on setup pages after 15 minutes	Yes	No
IPv6 on local probe/hosted probe	Yes	No
Single sign-on	Yes	No
Multi-factor authentication	No*	Yes

* PRTG Network Monitor supports multi-factor authentication with Microsoft Azure Active Directory and Okta.

- For more information, see the Knowledge Base: How can I enable Azure AD multi-factor authentication?
- For more information, see the Knowledge Base: How can I enable Okta multi-factor authentication?

Sensors on the Hosted Probe of PRTG Hosted Monitor

You can use the following sensors on the hosted probe of PRTG Hosted Monitor:

Supported Sensors
AWS Alarm v2 sensor

Supported Sensors
AWS Cost sensor
AWS EBS v2 sensor
AWS EC2 v2 sensor
AWS ELB v2 sensor
AWS RDS v2 sensor
Beckhoff IPC System Health sensor
Business Process sensor
Cisco IP SLA sensor
Citrix XenServer Host sensor
Citrix XenServer Virtual Machine sensor
Cloud HTTP v2 sensor
Cloud Ping v2 sensor
Cluster Health sensor
Common SaaS sensor
Core Health sensor
Dell EMC Unity Enclosure Health v2 sensor
Dell EMC Unity File System v2 sensor
Dell EMC Unity Storage Capacity v2 sensor
Dell EMC Unity Storage LUN v2 sensor
Dell EMC Unity Storage Pool v2 sensor
Dell EMC Unity VMware Datastore v2 sensor

Supported Sensors
DICOM Bandwidth sensor
DICOM C-ECHO sensor
DICOM Query/Retrieve sensor
DNS v2 sensor
Docker Container Status sensor
FortiGate System Statistics sensor
FTP sensor
FTP Server File Count sensor
HL7 sensor
HPE 3PAR Common Provisioning Group sensor
HPE 3PAR Drive Enclosure sensor
HPE 3PAR Virtual Volume sensor
HTTP sensor
HTTP Advanced sensor
HTTP Apache ModStatus PerfStats sensor
HTTP Apache ModStatus Totals sensor
HTTP Content sensor
HTTP Data Advanced sensor
HTTP IoT Push Data Advanced sensor
HTTP Transaction sensor
HTTP XML/REST Value sensor

Supported Sensors
IMAP sensor
IP on DNS Blacklist sensor
LDAP sensor
Microsoft 365 Mailbox sensor
Microsoft 365 Service Status sensor
Microsoft 365 Service Status Advanced sensor
Microsoft Azure SQL Database sensor
Microsoft Azure Storage Account sensor
Microsoft Azure Subscription Cost sensor
Microsoft Azure Virtual Machine sensor
Modbus TCP Custom sensor
MQTT Round Trip sensor
MQTT Statistics sensor
MQTT Subscribe Custom sensor
NetApp Aggregate sensor
NetApp I/O sensor
NetApp LIF sensor
NetApp LUN sensor
NetApp NIC sensor
NetApp Physical Disk sensor
NetApp SnapMirror sensor

Supported Sensors
NetApp System Health sensor
NetApp Volume sensor
NetApp Volume v2
OPC UA Certificate sensor
OPC UA Custom sensor
OPC UA Server Status sensor
Ping sensor
Ping Jitter sensor
POP3 sensor
Probe Health sensor
RADIUS v2 sensor
RDP (Remote Desktop) sensor
Redfish Power Supply sensor
Redfish System Health sensor
REST Custom sensor
Sensor Factory sensor
SFTP Secure File Transfer Protocol sensor
SIP Options Ping sensor
SMTP&IMAP Round Trip sensor
SMTP&POP3 Round Trip sensor
SNMP APC Hardware sensor

Supported Sensors
SNMP Buffalo TS System Health sensor
SNMP Cisco ADSL sensor
SNMP Cisco ASA VPN Connections sensor
SNMP Cisco ASA VPN Traffic sensor
SNMP Cisco ASA VPN Users sensor
SNMP Cisco CBQoS sensor
SNMP Cisco System Health sensor
SNMP Cisco UCS Blade sensor
SNMP Cisco UCS Chassis sensor
SNMP Cisco UCS Physical Disk sensor
SNMP Cisco UCS System Health sensor
SNMP CPU Load sensor
SNMP Custom sensor
SNMP Custom Advanced sensor
SNMP Custom String sensor
SNMP Custom String Lookup sensor
SNMP Custom Table sensor
SNMP Dell EqualLogic Logical Disk sensor
SNMP Dell EqualLogic Member Health sensor
SNMP Dell EqualLogic Physical Disk sensor
SNMP Dell Hardware sensor

Supported Sensors
SNMP Dell PowerEdge Physical Disk sensor
SNMP Dell PowerEdge System Health sensor
SNMP Disk Free sensor
SNMP Fujitsu System Health v2 sensor
SNMP Hardware Status sensor
SNMP HP LaserJet Hardware sensor
SNMP HPE BladeSystem Blade sensor
SNMP HPE BladeSystem Enclosure System Health sensor
SNMP HPE ProLiant Logical Disk sensor
SNMP HPE ProLiant Memory Controller sensor
SNMP HPE ProLiant Network Interface sensor
SNMP HPE ProLiant Physical Disk sensor
SNMP HPE ProLiant System Health sensor
SNMP IBM System X Logical Disk sensor
SNMP IBM System X Physical Disk sensor
SNMP IBM System X Physical Memory sensor
SNMP IBM System X System Health sensor
SNMP interSeptor Pro Environment sensor
SNMP Juniper NS System Health sensor
SNMP LenovoEMC Physical Disk sensor
SNMP LenovoEMC System Health sensor

Supported Sensors
SNMP Library sensor
SNMP Linux Disk Free sensor
SNMP Linux Load Average sensor
SNMP Linux Meminfo sensor
SNMP Linux Physical Disk sensor
SNMP Memory sensor
SNMP NetApp Disk Free sensor
SNMP NetApp Enclosure sensor
SNMP NetApp I/O sensor
SNMP NetApp License sensor
SNMP NetApp Logical Unit sensor
SNMP NetApp Network Interface sensor
SNMP NetApp System Health sensor
SNMP Nutanix Cluster Health sensor
SNMP Nutanix Hypervisor sensor
SNMP Poseidon Environment sensor
SNMP Printer sensor
SNMP QNAP Logical Disk sensor
SNMP QNAP Physical Disk sensor
SNMP QNAP System Health sensor
SNMP Rittal CMC III Hardware Status sensor

Supported Sensors
SNMP RMON sensor
SNMP SonicWall System Health sensor
SNMP SonicWall VPN Traffic sensor
SNMP Synology Logical Disk sensor
SNMP Synology Physical Disk sensor
SNMP Synology System Health sensor
SNMP System Uptime sensor
SNMP Traffic sensor
SNMP Windows Service sensor
SNTP sensor
Soffico Orchestra Channel Health sensor
SSH Disk Free sensor
SSH INodes Free sensor
SSH Load Average sensor
SSH Meminfo sensor
SSH Remote Ping sensor
SSH SAN Enclosure sensor
SSH SAN Logical Disk sensor
SSH SAN Physical Disk sensor
SSH SAN System Health sensor
SSH Script sensor

Supported Sensors
SSH Script Advanced sensor
SSL Certificate sensor
SSL Security Check sensor
System Health sensor
TFTP sensor
Traceroute Hop Count sensor
Veeam Backup Job Status sensor
Veeam Backup Job Status Advanced sensor
VMware Datastore (SOAP) sensor
VMware Host Hardware (WBEM) sensor
VMware Host Hardware Status (SOAP) sensor
VMware Host Performance (SOAP) sensor
VMware Virtual Machine (SOAP) sensor
Zoom Service Status sensor

Sensors on a Remote Probe Device

You can use the following sensors only on a remote probe 3621 device.

ⓘ For performance reasons, you cannot add these sensors to the hosted probe of PRTG Hosted Monitor.

Supported Sensors
Active Directory Replication Errors sensor
ADO SQL v2 sensor

Supported Sensors
Dell PowerVault MDi Logical Disk sensor
Dell PowerVault MDi Physical Disk sensor
DHCP sensor
Enterprise Virtual Array sensor
Event Log (Windows API) sensor
Exchange Backup (PowerShell) sensor
Exchange Database DAG (PowerShell) sensor
Exchange Database (PowerShell) sensor
Exchange Mailbox (PowerShell) sensor
Exchange Mail Queue (PowerShell) sensor
Exchange Public Folder (PowerShell) sensor
EXE/Script sensor
EXE/Script Advanced sensor
File sensor
File Content sensor
Folder sensor
HTTP Full Web Page sensor
HTTP Push Count sensor
HTTP Push Data sensor
HTTP Push Data Advanced sensor
Hyper-V Cluster Shared Volume Disk Free sensor

Supported Sensors
Hyper-V Host Server sensor
Hyper-V Virtual Machine sensor
Hyper-V Virtual Network Adapter sensor
Hyper-V Virtual Storage Device sensor
IPFIX sensor
IPFIX (Custom) sensor
IPMI System Health sensor
jFlow v5 sensor
jFlow v5 (Custom) sensor
Microsoft SQL v2 sensor
MySQL v2 sensor
NetFlow v5 sensor
NetFlow v5 (Custom) sensor
NetFlow v9 sensor
NetFlow v9 (Custom) sensor
Oracle SQL v2 sensor
Oracle Tablespace sensor
Packet Sniffer sensor
Packet Sniffer (Custom) sensor
PerfCounter Custom sensor
PerfCounter IIS Application Pool sensor

Supported Sensors
Port sensor
Port Range sensor
PostgreSQL sensor
Python Script Advanced sensor
QoS (Quality of Service) One Way sensor
QoS (Quality of Service) Round Trip sensor
sFlow sensor
sFlow (Custom) sensor
Share Disk Free sensor
SMTP sensor
SNMP Trap Receiver sensor
Syslog Receiver sensor
Windows CPU Load sensor
Windows IIS 6.0 SMTP Received sensor
Windows IIS 6.0 SMTP Sent sensor
Windows IIS Application sensor
Windows MSMQ Queue Length sensor
Windows Network Card sensor
Windows Pagefile sensor
Windows Physical Disk I/O sensor
Windows Print Queue sensor

Supported Sensors
Windows Process sensor
Windows System Uptime sensor
Windows Updates Status (PowerShell) sensor
WMI Battery sensor
WMI Custom sensor
WMI Custom String sensor
WMI Disk Health sensor
WMI Event Log sensor
WMI Exchange Server sensor
WMI Exchange Transport Queue sensor
WMI File sensor
WMI Free Disk Space (Multi Disk) sensor
WMI HDD Health sensor
WMI Logical Disk I/O sensor
WMI Memory sensor
WMI Microsoft SQL Server 2005 sensor (Deprecated)
WMI Microsoft SQL Server 2008 sensor
WMI Microsoft SQL Server 2012 sensor
WMI Microsoft SQL Server 2014 sensor
WMI Microsoft SQL Server 2016 sensor
WMI Microsoft SQL Server 2017 sensor

Supported Sensors
WMI Microsoft SQL Server 2019 sensor
WMI Remote Ping sensor
WMI Security Center sensor
WMI Service sensor
WMI Share sensor
WMI SharePoint Process sensor
WMI Storage Pool sensor
WMI Terminal Services (Windows 2008+) sensor
WMI Terminal Services (Windows XP/Vista/2003) sensor
WMI UTC Time sensor
WMI Vital System Data v2 sensor
WMI Volume sensor
WSUS Statistics sensor

Settings

These settings are only available in PRTG Network Monitor.

Setting Title	Setting Name
Auto-Update	When a New Version is Available
	Installation Time
	Release Channel
Notification Templates	Add Entry to Event Log

Setting Title	Setting Name
	Send Syslog Message
	Send SNMP Trap
	Execute Program
Core & Probes	Proxy Configuration
	Probe Connection IP Addresses
	Mini Probes
	Mini Probe Port
Administrative Tools For Probes	Restart Probe (local probe)
Scanning Intervals	Available Intervals (definition of individual intervals)
Notification Delivery	SMTP Delivery (everything but sender email address and name)
Recommended Sensors Detection	Detection Handling
User Interface (PRTG Web Interface)	DNS Name
	Google Analytics Tracking ID
User Interface (PRTG Web Server)	IP Address for PRTG Web Server
	TCP Port for PRTG Web Server
	PRTG Web Server Port
	PRTG Web Server Security
	Connection Security
	Active IP Address/Port Combinations
User Accounts	Login Name

Setting Title	Setting Name
	Password
	Passhash
Administrative Tools For The PRTG Core Server	Create Configuration Snapshot
	Write Core Status File
	Clear Caches
	Load Lookups and File Lists
	Recalculate PRTG Graph Data Cache
	Restart PRTG Core Server Service
	Reload Logging Configuration
Advanced Network Analysis	System Information
Scheduled Restart Settings (Local Probe)	Restart Options
	Restart Schedule
	Specify Day
	Specify Hour

15.2 Glossary

This section explains PRTG-specific terminology.

A

Alarms	The alarms list shows all sensors[3662] that are in the Down, Down (Partial), Down (Acknowledged), Warning, or Unusual status[3662]. The alarms list shows you all irregularities in your network.
Auto-discovery	The auto-discovery process uses ping to scan your network for devices[3662] (for groups[3662] only). It assesses the device type for all discovered devices, and it creates sensor[3662] sets that match the discovered device types based on built-in templates or your custom device templates[3662].

C

Channel	The monitoring data of a sensor[3662] is shown in channels. For example, sensors that measure network traffic have one channel each for traffic in, traffic out, and traffic total. You can set various triggers[3662] for each channel to define sensor status[3662] changes or notifications[3662] based on the monitoring data received.
Cluster	A cluster consists of two or more PRTG core servers[3662] that work together to form a high availability monitoring system. A cluster consists of a master node[3662] and one or more failover nodes[3662]. Every cluster node[3662] can monitor every device[3662] in a network for fail-safe monitoring.
Cluster node	Cluster nodes make up a cluster. Cluster nodes can be master nodes[3662] or failover nodes[3662].
Cluster probe	When you create or join a cluster[3662], PRTG automatically creates a cluster probe. All objects[3662] that you create on the cluster probe (or below in the device tree[3662]) are monitored by all cluster nodes[3662]. Create or move objects[3662] there for fail-safe monitoring. If one cluster node fails, the other cluster nodes continue to monitor all objects. You can add groups[3662] and devices[3662] to the cluster probe. The cluster probe runs as part of the local probe[3662].
Cluster probe device	The cluster probe device is an internal system device that PRTG automatically adds to the cluster probe[3662]. It has access to the cluster node[3662] system and monitors its health parameters using several sensors[3662].

D

Dashboard	A preconfigured sample dashboard is available in the Home menu of the PRTG web interface. Dashboards provide an overview of the overall status of your monitoring configuration. You can create custom dashboards using the Maps 3662 feature.
Device	A device represents a physical or virtual component in your network that is reachable via an IP address. For a clear device tree 3662 structure, you usually create one device for each physical or virtual component that you want to monitor. You can add one or more sensors 3662 to a device.
Device template	If you want to add a specific device 3662 several times, you can create a device template from a device in the device tree 3662. When you create a device template, PRTG saves information for nearly all sensors 3662 on the device to a template file. You can later use the template file in combination with the auto-discovery 3662 (restrictions apply for a few sensor types).
Device tree	The configuration of PRTG is represented in a hierarchical tree structure called the device tree, which contains all monitoring objects 3662. While building the device tree, you can relate to your network's topology to make your monitoring setup more understandable.

F

Failover master node	If the primary master node 3662 of a cluster 3662 fails, a failover node 3662 becomes a failover master node. The failover master node takes over the role of the primary master node until it reconnects to the cluster.
Failover node	In a cluster 3662, a failover node monitors all sensors 3662 on the cluster probe 3662 and it provides monitoring data for the PRTG core server 3662. Additionally, it serves as a backup in case the master node 3662 fails.
Flows	PRTG supports NetFlow v5, NetFlow v9, IPFIX, sFlow v5, and jFlow v5.

G

Gauge	A gauge is a type of visual representation of the values of a channel 3662. The gauge needle points to the current value of the channel. Other types of visual representations are toggles 3662 and switches 3662.
Geo Maps	The Geo Maps feature shows the different locations of your devices 3662 on a geographical map using the location data that you provide in the settings of probes 3662, groups 3662, or devices. The status icons on the geographical maps that represent your devices also show the overall status of a location. This is useful for monitoring distributed networks.

Group	A group is an organizational unit in the device tree. You can add devices or subgroups to groups. This way, you can model your physical network's topology within the PRTG configuration. You can use groups to arrange similar objects so that they inherit the same settings.

H

Hosted probe	The hosted probe in PRTG Hosted Monitor is like the local probe in PRTG Network Monitor. When you create a PRTG Hosted Monitor instance, the system automatically adds the hosted probe. The hosted probe runs on the PRTG core server system that we host for you and it shows the monitoring values of your PRTG Hosted Monitor instance. You can use the hosted probe to monitor devices, servers, and services that are publicly available on the internet like, for example, websites. To monitor your LAN, you need at least one remote probe installation in your network. The local probe is not available in PRTG Hosted Monitor.

L

Library	A library enables you to create additional views of your device tree. These views are updated in the same scanning interval as your device tree and show the same monitoring data, but arranged the way you want. This is useful if you want to display data in different ways, like depending on target groups or a specific use case.
Library node	Libraries use library nodes to reference objects in your monitoring setup. Library nodes can show a subtree of the device tree or they can show a collection of filtered sensors.
Limit	Limits let you define thresholds for channel values. When the value of a channel is above or below the defined limit, the sensor can show the Warning or Down status.
Local probe	When installing PRTG Network Monitor, the local probe is installed together with the PRTG core server. All objects created on the local probe, or underneath it in the device tree, are monitored by the local PRTG core server system. You can add groups and devices to the local probe. If you use PRTG Hosted Monitor, the hosted probe replaces the local probe.
Lookup	PRTG uses lookups for some sensor types and for some sensors with custom channels. In general, lookups map status values as returned by a device (usually integers) to more informative expressions in words.

M

Maps	The Maps feature lets you present monitoring data the way you want it. An editor is available that lets you create maps (sometimes referred to as dashboards[3662]) directly in your browser. Using maps, you can also make overviews of live data publicly available.
Master node	In a cluster[3662], the master node controls the settings and cluster management. It also takes over notifications. All changes to the monitoring configuration are made on the master node, which distributes the changes among all other cluster nodes in real time. There are two types of master nodes: primary master node[3662] and failover master node[3662].
Meta-scan	Sensors that use the meta-scan feature, for example SNMP sensors, first look at the according device[3662] to find what they can monitor. This can be tables, object identifiers (OID), or disks, for example. When the meta-scan is finished, the second step of the Add Sensor[413] dialog shows you the parameters that you can monitor. Some sensors require basic information before they can perform a meta-scan. Provide the requested information, such as credentials, in the appearing dialog box. PRTG then scans and recognizes all parameters that are available for monitoring based on your input.
Mini probe	With a mini probe, you can create small probes[3662] on any device[3662] (not only on Windows systems).

N

Notification	PRTG uses notifications to send you alerts whenever it discovers a defined status, such as slow sensors[3662], or when channels[3662] breach threshold values. You can define an unlimited number of notifications. You can use one or more of several notification methods like email, text messaging, push notifications to Android and iOS devices, and more.
Notification trigger	PRTG sends a notification[3662] when a defined event triggers it. These events are known as notification triggers. The following events can trigger notifications: sensor status[3662] changes, sensor[3662] value threshold breaches, speed threshold breaches, volume threshold breaches, and sensor value changes.

O

Object	All types of items in the device tree[3662] are generally referred to as objects, or monitoring objects. An object can be a probe[3662], a group[3662], a device[3662], or a sensor[3662].

Object hierarchy	All objects 3662 are arranged in a hierarchical order called the object hierarchy. The object hierarchy is used to define common settings for groups of objects.
Object selector	The object selector lets you browse all objects 3662 in your configuration and lets you select an object. The left-hand side shows the device tree 3662. If you have selected a device 3662, the right-hand side shows the sensors 3662 on the device.

P

Primary group	Every user has to be a member of a primary group to make sure there is no user without group membership. Membership in other user groups is optional.
Primary master node	In a cluster 3662, the primary master node is the cluster node 3662 that is the master node 3662 by configuration.
Probe	A probe is where the actual monitoring takes place. There are local probes 3662, cluster probes 3662, remote probes 3662, and hosted probes 3662.
Probe device	The probe device is an internal system device that PRTG automatically adds to the local probe 3662. It has access to the probe system 3662 and monitors its health parameters using several sensors 3662.
Probe system	A probe system is the system, or Windows computer, that runs a probe 3662. A remote probe 3662, a cluster probe 3662, and the local probe 3662 run on a probe system.
PRTG Administration Tool	The PRTG Administration Tool is part of your PRTG installation. You can use it to edit the administrative settings of the local probe 3662 and remote probe 3662 installations. You can start the PRTG Administration Tool from the Windows Start menu on the PRTG core server system 3662 or on the remote probe system 3662.
PRTG Application Programming Interface (PRTG API)	The PRTG API enables you to access monitoring data and to manipulate objects 3662 using HTTP requests, to run your own written sensors 3662 and notifications 3662, and to implement mini probes 3662.
PRTG Cloud	The PRTG Cloud is used by the Cloud HTTP v2 sensor and the Cloud Ping v2 sensor to monitor the loading times of a web server via HTTP or the Transmission Control Protocol (TCP) ping times to a parent device from different locations worldwide. PRTG also sends push notifications and securely transmits support bundles to Paessler via the PRTG Cloud.

PRTG core server	The PRTG core server is the central unit of PRTG. It receives monitoring data from the probe and handles reporting and notifications, provides the web server for the user interfaces, and much more. In a cluster, one PRTG core server is installed on every cluster node. The PRTG core server is configured as a Windows service that is permanently run by the Windows system without requiring a user that is logged in.
PRTG core server service	The PRTG core server service is responsible for running the PRTG core server. It is a Windows service that permanently runs on the PRTG core server system.
PRTG core server system	The PRTG core server system is the system, or Windows computer, that runs the PRTG core server.
PRTG data directory	The PRTG data directory is the directory on the PRTG core server system or remote probe system where PRTG stores monitoring data, configuration data, and logs.
PRTG Desktop	PRTG Desktop is an alternative interface that you can use to connect to the PRTG core server or a PRTG Hosted Monitor instance to configure your setup, view monitoring results, and keep an eye on your network. It is a cross-platform application for fast access to data and monitoring management.
PRTG Hosted Monitor	PRTG Hosted Monitor is the PRTG cloud solution where we at Paessler run the PRTG core server and hosted probe for you. PRTG Hosted Monitor does not require a PRTG core server installation inside your network.
PRTG Network Monitor	PRTG Network Monitor is a network monitoring application for Windows-based systems with which you can monitor your entire network. PRTG Network Monitor requires a PRTG core server installation inside your network.
PRTG probe service	The PRTG probe service is responsible for running a probe. It is a Windows service that permanently runs on the probe system.
PRTG program directory	The PRTG program directory is the directory on the PRTG core server system where PRTG stores all files that are required for it to run.
PRTG web interface	The PRTG web interface is the Asynchronous JavaScript and XML (AJAX) based web interface of PRTG. It is the default interface for setting up your monitoring.

R

Recommended Sensors Detection	The Recommended Sensors Detection feature enables PRTG to analyze devices 3662 in your network and to suggest sensors that are still missing for a comprehensive monitoring setup. If enabled, the analysis runs in the background with low priority if you add a new device, if the last analysis was executed more than 30 days ago, or if you manually start it.
Release channel	PRTG updates are delivered in different release channels. With PRTG Network Monitor, you can choose between maximum stability (Stable), or most early access to new features (Canary or Preview). PRTG Hosted Monitor does not have release channels. Instead, we roll out the latest stable version to PRTG Hosted Monitor instances in stages, so your instance automatically updates to the latest stable version.
Remote probe	A remote probe is a small piece of software that is installed on a computer, or remote probe system 3662, in the local or remote network. It scans the network and sends monitoring results to the PRTG core server 3662. Once the connection has been established, the remote probe is shown in the device tree 3662. All objects 3662 that you create on the remote probe, or below it in the device tree, are monitored by the remote probe system. You can add groups 3662 and devices 3662 to the remote probe. In a cluster 3662, remote probes can connect to all cluster nodes so you can view monitoring data of a remote probe on all cluster nodes 3662.
Remote probe device	The remote probe device is an internal system device that PRTG automatically adds to the remote probe 3662. It has access to the remote probe system 3662 and monitors its health parameters using several sensors 3662.
Remote probe system	The remote probe system is the system, or Windows computer, that runs a remote probe 3662.
Root group	The root group is the topmost instance in the object hierarchy 3662 in the device tree. It contains all objects 3662 in your monitoring setup. All objects inherit the settings of the root group by default.

S

Schedule	You can use schedules to pause monitoring or notifications for certain periods of time or at certain times. You can also use schedules to define the periods of time that are covered when creating reports.
Sensor	A sensor monitors one aspect of a device 3662. For example, one sensor monitors if a device responds to a ping request. A different sensor monitors the traffic of one Ethernet port of a router, and so on. The data of sensors is shown in their respective channels 3662. Each sensor has at least one channel.

Sensor status	The color of a sensor 3662 represents the sensor status. There are 8 different sensor states: Down, Down (Partial), Down (Acknowledged), Warning, Unusual, Up, Paused, and Unknown.
Similar Sensors Detection	The Similar Sensors Detection feature enables PRTG to analyze sensor 3662 data for similarities. If enabled, the detection runs in the background with low priority. The recommended setting for the analysis depth is to let PRTG automatically decide how many channels 3662 it analyzes.
Switch	A switch is a type of visual representation of the values of a channel 3662. Switches represent boolean values when using lookups 3662.

T

Tickets	Tickets are created by the system or by a user and contain important messages or action steps for the administrator or other users to take. You should view every ticket 211 to take appropriate action. You can access the list of tickets from the main menu.
Toggle	A toggle is a type of visual representation of the values of a channel 3662. Toggles represent bitfields when using lookups 3662.
Toplist	Packet Sniffer and Flow (NetFlow, jFlow, sFlow, IPFIX) sensor 3662 types can break down traffic by IP address, port, protocol, and other parameters. The results are shown in graphs that are called Toplists.

U

Unusual Detection	The Unusual Detection feature can set sensors 3662 to the Unusual status 3662 when it detects values that are not typical for the time span in which they are measured. If the detection is enabled, PRTG compares the current average values to the historic monitoring results for this purpose. If the current values show a big difference to the values that are normally retrieved by a sensor, this sensor indicates this with the Unusual status.

15.3 Legal Notices

See below for an excerpt of the libraries and licenses that PRTG uses.

- Build using Indy Internet Direct (https://www.indyproject.org/).
  This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
- Uses the net-SNMP library, see netsnmp-license.txt
- Uses Python under the Python Software Foundation License (https://docs.python.org/3.7/license.html#psf-license-agreement-for-python-release)
- Uses NexusMM (https://www.nexusdb.com/)
- Delphi Chromium Embedded (https://code.google.com/archive/p/delphichromiumembedded/) under the Mozilla Public License 1.1 (MPL 1.1, available from http://www.mozilla.org/en-US/MPL/1.1/)
- Soundfiles from https://www.soundsnap.com/
- Uses Public Domain regional maps from "The World Factbook 2016-17" Washington, DC: Central Intelligence Agency, 2016 (https://www.cia.gov/library/publications/the-world-factbook/docs/refmaps.html)
- Icons from https://www.androidicons.com/
- Uses the IPMIUTIL library under the BSD 2.0 license, see ipmi_bsd-2.0.txt
- Uses PhantomJS, see phantomjs-license.bsd
- Uses the Npgsql .Net Data Provider for Postgresql library (for license information see ipmi_bsd-2.0.txt)
- Uses NPcap (https://nmap.org/npcap/oem/redist.html)
- Uses GeoLite2 data created by MaxMind (https://www.maxmind.com)

Code libraries using

- MIT (https://opensource.org/licenses/MIT)
- MPL 1.1 (https://www.mozilla.org/media/MPL/1.1/index.0c5913925d40.txt)
- MPL 2.0 (https://www.mozilla.org/media/MPL/2.0/index.815ca599c9df.txt)
- APL 2.0 (https://www.apache.org/licenses/LICENSE-2.0.txt)
- BSD 2.0 license (https://opensource.org/licenses/BSD-2-Clause)
- BSD 3.0 license (https://opensource.org/licenses/BSD-3-Clause)

Licenses used in previous versions of PRTG:

- FastMM (https://sourceforge.net/projects/fastmm/)
- TPLockBox (https://sourceforge.net/projects/tplockbox/)
- "wkhtmltopdf" (https://wkhtmltopdf.org/) library distributed under the GNU LESSER GENERAL PUBLIC LICENSE (see wkhtmltopdf_lgpl-3.0.txt)
- WinPcap (https://www.winpcap.org/misc/copyright.htm)

Privacy Policy

https://www.paessler.com/company/privacypolicy

Terms and Conditions

https://www.paessler.com/company/terms

Last manual export: Monday, May 22, 2023 5:34:32 AM

15.4 List of Abbreviations

See below for a list of abbreviations used in this documentation.

A

ACL	access control list
AD	Active Directory
ADO	ActiveX Data Objects
ADSL	asymmetric digital subscriber line
AES	Advanced Encryption Standard
AET	Application Entity Title
AIM	AOL Instant Messenger
AJAX	Asynchronous JavaScript and XML
API	application programming interface
ARP	Address Resolution Protocol
AWS	Amazon Web Services
Azure AD	Azure Active Directory

B

BA	basic authentication
BMC	Baseboard Management Controller

C

CA	certificate authority
CBQoS	Class Based Quality of Service
CGI	Common Gateway Interface

CIFS	Common Internet File System
CLI	command-line interface
CLR	common language runtime
COM	component object model
CPG	Common Provisioning Group
CRC	cyclic redundancy check
CSP	cloud solution provider
CSV	comma-separated values

D

DAE	disk-array enclosure
DAG	Database Availability Group
DBMS	database management system
DC	domain controller
DCS	domain components
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DN	distinguished name
DNS	Domain Name System
DoS	denial of service
DPE	disk processor enclosure
DSCP	Differentiated Services Code Point

DTU	Database Transaction Unit

E

EBS	Elastic Block Store
EC2	Elastic Compute Cloud
ECC	Elliptic Curve Cryptography
eDTU	elastic Database Transaction Unit
ELB	Elastic Load Balancing
EVA	Enterprise Virtual Array

F

FAT	file allocation table
FCP	Fibre Channel Protocol
FCS	Frame Check Sequence
FIPS	Federal Information Processing Standards
Flow	Flow (NetFlow, jFlow, sFlow, IPFIX)
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FTPS	FTP over SSL

G

GID	global ID
GUID	globally unique identifier

H

HL7	Health Level 7
HTTP	Hypertext Transfer Protocol

I

I/O	input/output
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICPIF	Impairment Calculated Planning Impairment Factor
IDE	integrated development environment
iDRAC	Integrated Dell Remote Access Controller
IIS	Microsoft Internet Information Services
IKE	Internet Key Exchange
iLO	HPE Integrated Lights Out
IMAP	Internet Message Access Protocol
IMM	Integrated Management Module
IOPS	input/output operations per second
IoT	Internet of Things
IPC	Industrial PC
IPFIX	Internet Protocol Flow Information Export
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
IRC	Internet Relay Chat

iRMC	integrated Remote Management Controller
iSCSI	Internet Small Computer System Interface

J

JSON	JavaScript Object Notation
JWKS	JSON Web Key Set

L

L2L	LAN-to-LAN
LCU	load balancer capacity units
LDAP	Lightweight Directory Access Protocol
LIF	logical interface
LUN	logical unit number

M

MD5	message-digest algorithm 5
MIB	Management Information Base
MOID	managed object identifier
MOS	mean opinion score
MQTT	Message Queue Telemetry Transport
ms	milliseconds
msec	milliseconds
MSH	message header
MSMQ	Microsoft Message Queuing

MSP	managed service provider
mutex	mutual exclusion
MWL	Modality Worklist

N

NAS	network-attached storage
NAT	network address translation
NFS	network file system
NIC	network interface card
Nmap	Network Mapper
NSA	Network Security Appliance
NTFS	New Technology File System
NTLM	NT LAN Manager

O

OAuth2	Open Authorization 2
ODBC	Open Database Connectivity
OID	object identifier
OMSA	OpenManage Server Administrator
ONTAPI	DATA ONTAP API
OPC UA	OPC Unified Architecture
OSPF	Open Shortest Path First
OU	organizational unit

P

P2P	Peer-to-Peer
PACS	picture archiving and communication system
PAP	Password Authentication Protocol
PCRE	Perl Compatible Regular Expression
PDV	packet delay variation
PEM	Privacy-Enhanced Mail
PMPP	PRTG Mini Probe Protocol
POP3	Post Office Protocol version 3
PRTG	PRTG Network Monitor; Paessler PRTG Enterprise Monitor

Q

QNAP	Quality Network Appliance Provider
QoS	Quality of Service

R

RADIUS	Remote Authentication Dial-In User Service
RAID	redundant array of independent disks
RDP	Remote Desktop Protocol
RDS	Relational Database Service
Redfish	Redfish Scalable Platforms Management API
regex	regular expression
REST	Representational State Transfer

RMON	Remote Monitoring
RODC	Read-only Domain Controllers
RPC	remote procedure call
RPM	revolutions per minute
RST	number of reset
RTT	round-trip time
RTU	Remote Terminal Unit

S

S.M.A.R.T.	Self-Monitoring, Analysis and Reporting Technology
SaaS	software as a service
SAN	storage area network
SASL	Simple Authentication and Security Layer
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SID	Oracle System ID
SIP	Session Initiation Protocol
SLA	service level agreement
SMB	server message block
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SNMP	Simple Network Management Protocol
SNR	signal-to-noise ratio

SNS	Simple Notification Service
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SPA	Single Page Application
SPAN	Switched Port Analyzer
SPN	Service Principal Name
SQL	Structured Query Language
SRP	Secure Remote Password
SSD	solid-state drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	single sign-on
SVC	switched virtual circuit

T

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ToS	Type of Service
TOTP	Time-based One-time Password algorithm

U

UAC	User Account Control

UCS	Unified Computing System
UDF	User-defined Function
UDP	User Datagram Protocol
UID	Unique Identifier
UNC	Universal Naming Convention
UPS	uninterruptible power supplies
URI	uniform resource identifier
UTC	Coordinated Universal Time
UUID	universally unique identifier

V

vCore	virtual core
VM	virtual machine
VNC	Virtual Network Computing
VoIP	Voice over IP
VPN	virtual private network

W

WBEM	Web-based Enterprise Management
WMI	Windows Management Instrumentation
WQL	Windows Management Instrumentation Query Language
WSAPI	Web Services API
WSUS	Windows Server Update Services

WWN	World Wide Name

X

XML	Extensible Markup Language
XSS	cross-site scripting

15.5 List of Available Sensor Types

Here you can find a list of all available sensors, including their category, the version they were introduced in, their performance impact, IP version, meta-scan capability, device template capability, notification triggers, and what they monitor.

ⓘ In the Add a Sensor 413 assistant, you have various options to filter for suitable sensors. You can also filter for device template capability, IP version, and meta-scan functionality, among others, via /sensorlist.htm, for example https://yourserver/sensorlist.htm.

In this section:

General

General sensors let you monitor the basic parameters of your network.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Cloud HTTP v2 Response time and response code of the target server via HTTP	20.3.62		No	No	No	State Threshold
Cloud Ping v2 Response time of the target server via TCP ping	20.3.62		Yes	No	No	State Threshold
HTTP	7		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Loading time of a web page or element						
Ping Ping time and packet loss	7		No	No	Yes	State Threshold
Port Time until a request to a port is accepted	7		No	No	Yes	State Threshold
Port Range Network service by connecting to various TCP/IP ports	12.x.4		No	No	Yes	State Threshold Change
SNMP Traffic Traffic on a device via SNMP	7		No	Yes	Yes	State Speed Volume
SSL Certificate Certificate of an SSL/TLS connection	15.x.19		No	No	Yes	State Threshold
SSL Security Check SSL/TLS connectivity to the port of a device	14.x.12		No	No	Yes	State Threshold
Windows Network Card Bandwidth usage and traffic of a network interface via WMI or Windows performance counters	7		No	Yes	Yes	State Speed Volume

Backup and replication monitoring

Backup and replication monitoring sensors let you monitor backup and replication jobs.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Active Directory Replication Errors Windows DC for replication errors	8.3.0		No	Yes	Yes	State Threshold Change
File Changes to file content and file time stamp	7		No	No	Yes	State Threshold Change
Folder Folder via SMB	7		No	No	Yes	State Threshold Change
IMAP Email server via IMAP	7		Yes	No	Yes	State Threshold
Veeam Backup Job Status Status of all backup job runs on the Veeam Backup Enterprise Manager in the last 24 hours	20.4.64		No	No	Yes	State Threshold
Veeam Backup Job Status Advanced Status of a specific backup job that runs on the Veeam Backup Enterprise Manager	21.x.69		No	Yes	Yes	State Threshold

Bandwidth monitoring

Bandwidth monitoring sensors let you analyze your network bandwidth.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
IPFIX Traffic data from an IPFIX-compatible device	13.x.7		Yes	No	No	State Speed Volume
IPFIX (Custom) Traffic data from an IPFIX-compatible device	13.x.7		Yes	No	No	State Speed Volume
jFlow v5 Traffic data from a jFlow v5 compatible device	8.2.0		Yes	No	No	State Speed Volume
jFlow v5 (Custom) Traffic data from a jFlow v5 compatible device	8.2.0		Yes	No	No	State Speed Volume
NetFlow v5 Traffic data from a NetFlow v5 compatible device	7		No	No	No	State Speed Volume
NetFlow v5 (Custom) Traffic data from a NetFlow v5 compatible device	7		No	No	No	State Speed Volume
NetFlow v9 Traffic data from a NetFlow v9 compatible device	7		No	No	No	State Speed Volume
NetFlow v9 (Custom) Traffic data from a NetFlow v9 compatible device	7		No	No	No	State Speed Volume

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Packet Sniffer Headers of data packets that pass a local network card	7		No	No	No	State Speed Volume
Packet Sniffer (Custom) Headers of data packets that pass a local network card	7		No	No	No	State Speed Volume
sFlow Traffic data from an sFlow v5 compatible device	7		Yes	No	No	State Speed Volume
sFlow (Custom) Traffic data from an sFlow v5 compatible device	7		Yes	No	No	State Speed Volume
SNMP Cisco ADSL ADSL statistics of a Cisco router	12.x.1		No	Yes	Yes	State Threshold
SNMP Cisco ASA VPN Traffic Traffic of an IPsec VPN connection on a Cisco ASA	12.x.1		No	Yes	Yes	State Speed Volume
SNMP HPE ProLiant Network Interface Network interface in an HPE server via SNMP	12.x.4		No	Yes	Yes	State Speed Volume
SNMP Library Device via SNMP	7		No	Yes	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
SNMP NetApp Network Interface Network card of a NetApp storage system via SNMP	12.x.3		No	Yes	Yes	State Speed Volume
SNMP RMON Traffic on a device using RMON via SNMP	12.x.1		No	Yes	Yes	State Speed Volume
SNMP SonicWall VPN Traffic Traffic of an IPsec VPN on a SonicWall NSA via SNMP	13.x.6		No	Yes	Yes	State Speed Volume
SNMP Traffic Traffic on a device via SNMP	7		No	Yes	Yes	State Speed Volume
Windows Network Card Bandwidth usage and traffic of a network interface via WMI or Windows performance counters	7		No	Yes	Yes	State Speed Volume

Beta sensors

Here you can find a list of sensors that are currently in the beta status.

ⓘ To use beta sensors, enable the Beta Sensors experimental feature of PRTG. For more information, see the Knowledge Base: What are beta sensors and how can I use them?

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Cisco Meraki License Meraki licenses of an organization via the Cisco Meraki Dashboard API	N/A		No	Yes	Yes	State Threshold
Cisco Meraki Network Health Health of Cisco Meraki network devices via the Cisco Meraki Dashboard API	N/A		No	Yes	Yes	State Threshold
FortiGate VPN Overview The VPN connections of a Fortinet FortiGate system via the REST API	N/A		No	No	Yes	State Threshold
HTTP v2 A web page or an element of a web page	N/A		No	No	Yes	State Threshold
Local Folder A local folder on a probe system	N/A		No	No	No	State Threshold
Network Share A SMB or CIFS network share	N/A		No	No	No	State Threshold
Ping v2 Availability of the target, ping time, and packet loss	N/A		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Port v2 Network service by connecting to various TCP/IP ports	N/A		No	No	Yes	State Threshold
Redfish Virtual Disk Virtual disk of a Redfish-capable server	N/A		No	Yes	Yes	State Threshold
REST Custom v2 A JSON or XML REST API endpoint and maps the JSON or XML result to sensor values	N/A		No	Yes	No	State Threshold
Script v2 Values returned by the Python script in multiple channels	N/A		No	Yes	Yes	State Threshold
SNMP Custom v2 Single parameter that is returned by a specific OID or ASN.1 MIB via SNMP	N/A		No	No	No	State Threshold
SNMP Uptime v2 Uptime of a device via SNMP	N/A		No	No	No	State Threshold

Cloud service

Cloud service sensors let you get a quick overview of all cloud services.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
AWS Alarm v2 Status of an AWS alarm by reading its data from Amazon CloudWatch via the AWS API	22.x.76		No	Yes	Yes	State Threshold
AWS Cost Cost of an AWS account by reading its data from the AWS Cost Explorer API	20.1.56		No	No	Yes	State Threshold
AWS EBS v2 Performance of an AWS EBS volume by reading its data from Amazon CloudWatch via the AWS API	22.x.76		No	Yes	Yes	State Threshold
AWS EC2 v2 Performance of an AWS EC2 instance by reading its data from Amazon CloudWatch via the AWS API	22.x.76		No	Yes	Yes	State Threshold
AWS ELB v2 Performance of an AWS ELB load balancer by reading its data from Amazon CloudWatch via the AWS API	22.x.76		No	Yes	Yes	State Threshold
AWS RDS v2 Performance of a AWS RDS instance by reading its data from Amazon CloudWatch via the AWS API	22.x.77		No	No	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Common SaaS Availability of several SaaS providers	15.x.19		No	No	Yes	State Threshold
Microsoft 365 Mailbox A Microsoft 365 mailbox folder	22.x.79		No	Yes	No	State Threshold
Microsoft 365 Service Status Overall status of all services of a Microsoft 365 subscription	20.3.61		No	No	Yes	State Threshold
Microsoft 365 Service Status Advanced Detailed status of a service of a Microsoft 365 subscription	20.3.61		No	Yes	Yes	State Threshold
Microsoft Azure SQL Database Metrics of an Azure SQL Database (single database or elastic pool) in a Microsoft Azure subscription	21.x.70		No	Yes	Yes	State Threshold
Microsoft Azure Storage Account Storage account in a Microsoft Azure subscription	21.x.70		No	Yes	Yes	State Threshold
Microsoft Azure Subscription Cost Cost in a Microsoft Azure subscription	20.4.64		No	No	Yes	State Threshold
Zoom Service Status	20.3.61		No	No	Yes	State

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Availability of global Zoom services						Threshold

Custom

Custom sensors let you enhance the monitoring task far beyond the standard sensor set.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Business Process Summarized status of entire business processes while monitoring several process components	15.x.20		No	No	No	State Threshold
EXE/Script Value returned by the executable file or script (in one channel only) and the execution time	7		No	Yes	Yes	State Threshold Change
EXE/Script Advanced Values returned by the executable file or script in multiple channels	7		No	Yes	Yes	State Threshold Change
IPFIX (Custom) Traffic data from an IPFIX-compatible device	13.x.7		Yes	No	No	State Speed Volume
jFlow v5 (Custom) Traffic data from a jFlow v5 compatible device	8.2.0		Yes	No	No	State Speed Volume

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
NetFlow v5 (Custom) Traffic data from a NetFlow v5 compatible device	7		No	No	No	State Speed Volume
NetFlow v9 (Custom) Traffic data from a NetFlow v9 compatible device	7		No	No	No	State Speed Volume
Packet Sniffer (Custom) Headers of data packets that pass a local network card	7		No	No	No	State Speed Volume
Python Script Advanced Values returned by the Python script in multiple channels	15.x.19		No	Yes	Yes	State Threshold
REST Custom Values returned by a REST API in multiple channels	17.3.33		No	Yes	No	State Threshold
Sensor Factory Entire business processes that involve several components	7		No	No	No	State Threshold
sFlow (Custom) Traffic data from an sFlow v5 compatible device	7		Yes	No	No	State Speed Volume
SNMP Custom	7		No	No	Yes	State Threshold Change

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Single parameter that is returned by a specific OID via SNMP						
SNMP Custom Advanced Numeric values returned for OIDs via SNMP	15.x.18		No	No	Yes	State Threshold
SNMP Custom String String returned by a specific OID via SNMP	9.1.0		No	No	Yes	State Threshold Change
SNMP Custom String Lookup String returned by a specific OID via SNMP directly mapped to a sensor status	14.x.14		No	Yes	Yes	State Threshold
SNMP Custom Table Entries from a table that is provided via SNMP	15.x.18		No	Yes	Yes	State Threshold
SSH Script Value returned by the executable file or script (in one channel only) and the execution time	12.x.1		Yes	Yes	Yes	State Threshold Change
SSH Script Advanced Values returned by the script in multiple channels and the execution time	12.x.6		Yes	Yes	Yes	State Threshold Change

Database server

Database server sensors let you monitor the most common databases.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
ADO SQL v2 Database via an ADO connection	16.x.24		No	Yes	Yes	State Threshold Change
Microsoft SQL v2 Database on a Microsoft SQL server	14.x.12		No	Yes	Yes	State Threshold Change
MySQL v2 Database on a MySQL server	14.x.12		No	Yes	Yes	State Threshold Change
Oracle SQL v2 Database on an Oracle server	14.x.13		No	Yes	Yes	State Threshold Change
Oracle Tablespace Tablespace on an Oracle server	15.x.18		No	Yes	Yes	State Threshold Change
PostgreSQL Database on a PostgreSQL server	14.x.12		No	Yes	Yes	State Threshold Change
WMI Microsoft SQL Server 2005 Performance of a Microsoft SQL Server via WMI	8.1.0		No	No	Yes	State Threshold
WMI Microsoft SQL Server 2008	8.1.0		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Performance of a Microsoft SQL Server via WMI						
WMI Microsoft SQL Server 2012 Performance of a Microsoft SQL Server via WMI	12.x.6		No	Yes	Yes	State Threshold
WMI Microsoft SQL Server 2014 Performance of a Microsoft SQL Server via WMI	14.x.13		No	Yes	Yes	State Threshold
WMI Microsoft SQL Server 2016 Performance of a Microsoft SQL Server via WMI	16.x.26		No	Yes	Yes	State Threshold
WMI Microsoft SQL Server 2017 Performance of a Microsoft SQL Server via WMI	18.x.42		No	Yes	Yes	State Threshold
WMI Microsoft SQL Server 2019 Performance of a Microsoft SQL Server via WMI	20.3.62		No	Yes	Yes	State Threshold

eHealth

eHealth sensors let you monitor medical equipment.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
DICOM Bandwidth Bandwidth usage of a C-STORE request to a DICOM-capable device	18.1.38		No	No	No	State Threshold Change
DICOM C-ECHO Availability of DICOM-capable systems and devices by sending C-ECHO requests to the target system	18.1.38		No	No	No	State Threshold Change
DICOM Query/Retrieve C-FIND capability of DICOM-capable systems and devices	18.1.38		No	No	No	State Threshold Change
Soffico Orchestra Channel Health State and overall number of successful or failed channel calls	20.4.63		No	Yes	No	State Threshold

EXE

EXE sensors let you carry out a wide range of different operations.

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Active Directory Replication Errors Windows DC for replication errors	8.3.0		No	Yes	Yes	State Threshold Change
ADO SQL v2	16.x.24		No	Yes	Yes	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Database via an ADO connection						Change
Citrix XenServer Host Xen host server via HTTP	12.x.1		Yes	Yes	Yes	State Threshold Change
Citrix XenServer Virtual Machine VM on a Citrix XenServer via HTTP	8.1.0		Yes	Yes	Yes	State Threshold Change
Dell PowerVault MDi Logical Disk Virtual disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, MD3620f, or MD3820i	12.x.1		Yes	Yes	Yes	State Threshold
Dell PowerVault MDi Physical Disk Physical disk on a Dell PowerVault MD3000i, MD3420, MD3620i, MD3000f, or MD3620f	14.x.13		No	Yes	Yes	State Threshold
DICOM Bandwidth Bandwidth usage of a C-STORE request to a DICOM-capable device	18.1.38		No	No	No	State Threshold Change
DICOM C-ECHO	18.1.38		No	No	No	State Threshold

Sensor	As of PRTG	Perf. Impact	IPv4 Only	Meta-Scan	Device Template	Notification Trigger
Availability of DICOM-capable systems and devices by sending C-ECHO requests to the target system						Change
DICOM Query/Retrieve C-FIND capability of DICOM-capable systems and devices	18.1.38		No	No	No	State Threshold Change
Enterprise Virtual Array HPE Storage EVA via the sssu.exe from HPE P6000 Command View Software	13.x.6		No	Yes	No	State Threshold
Exchange Backup (PowerShell) Backups of an Exchange server via Remote PowerShell	13.x.5		Yes	Yes	No	State Threshold Change
Exchange Database (PowerShell) Database information of an Exchange server via Remote PowerShell	13.x.5		Yes	Yes	No	State Threshold Change
Exchange Database DAG (PowerShell)	15.x.18		Yes	Yes	No	State Threshold Change