Setting	Description
	ⓘ This setting is only relevant if you use WBEM sensors.
Custom WBEM Port	This setting is only visible if you select Custom above. Enter a custom WBEM port. Enter an integer.
SSH Port	Enter the port for SSH connections. Enter an integer. The default port is 22. ⓘ By default, PRTG automatically uses this setting for all SSH sensors[3683] unless you define a different port number in the sensor settings.
SSH Rights Elevation	Select the rights that you want to use to run the command on the target system: ▪ Run the command as the connecting user (default): Use the rights of the user who establishes the SSH connection. ▪ Run the command as a different user using 'sudo' (with password): Use the rights of a different user with a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'sudo' (without password): Use the rights of a different user without a password required for sudo to run commands on the target system, for example, as a root user. ▪ Run the command as a different user using 'su': Use the rights of a different user with su to run commands on the target system.
Target System User Name	This setting is only visible if you select an option that includes sudo or su above. Enter a user name to run the specified command on the target system as a different user than the root user. If you leave this field empty, you run the command as a root user. Make sure that you set the Linux password even if you use a public key or a private key for authentication. This is not necessary if the user is allowed to run the command without a password.
Password	This setting is only visible if you select an option that includes sudo or su with password above. Enter the password to run the sudo command or the su command.
SSH Connection Mode	Select the connection mode that you want to use to access data with SSH sensors[3437]: ▪ Default (recommended): This is the default connection mode for SSH sensors. It provides the best performance and security. ▪ Compatibility mode (deprecated): Use this only if the default connection mode does not work on the target system. The compatibility mode is the connection mode that PRTG used in previous versions and it is deprecated.

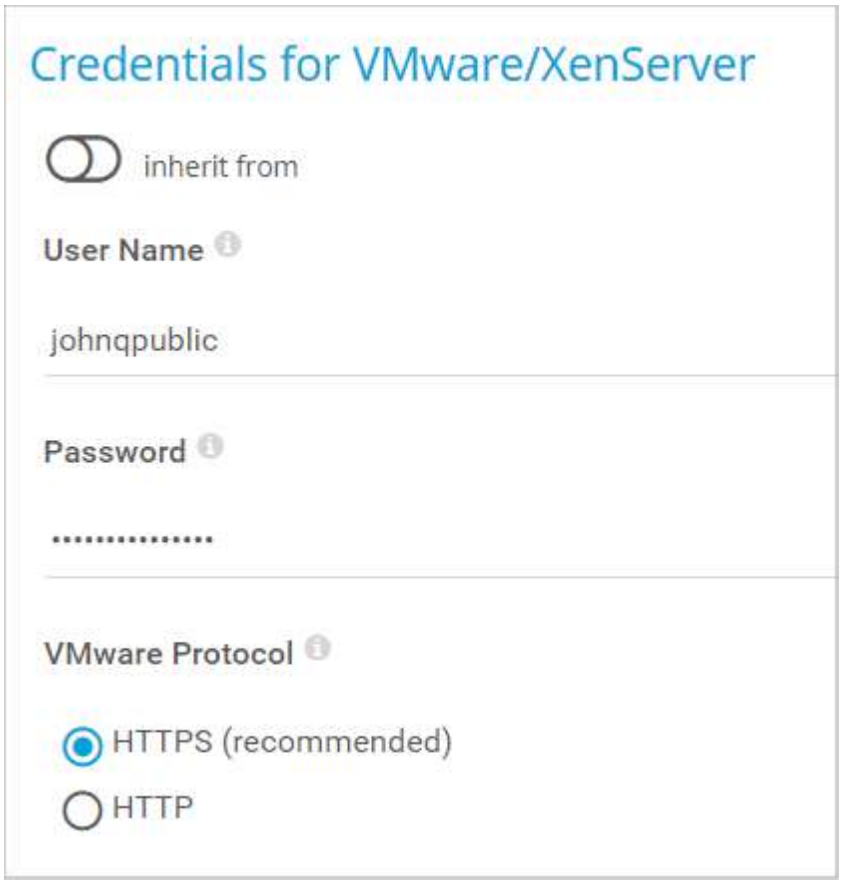
Setting	Description
	We strongly recommend that you use the default connection mode. You can also individually select the connection mode for each SSH sensor in the sensor settings.

Credentials for VMware/XenServer

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Citrix XenServer Host
- Citrix XenServer Virtual Machine
- VMware Datastore (SOAP)
- VMware Host Hardware (WBEM)
- VMware Host Hardware Status (SOAP)
- VMware Host Performance (SOAP)
- VMware Virtual Machine (SOAP)



Credentials for VMware/XenServer

Setting	Description
User Name	Enter the user name for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights.
Password	Enter the password for access to VMware ESXi, vCenter Server, or Citrix XenServer. Usually, you use credentials with administrator rights. ⓘ Single sign-on (SSO) passwords for vSphere do not support special characters. For details, see the VMware sensors sections.
VMware Protocol	Select the protocol for the connection to VMware ESXi, vCenter Server, or Citrix XenServer: ▪ HTTPS (recommended): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Session Handling	Select if you want to reuse a session for VMware sensors: ▪ Reuse a session for multiple scans (recommended): Select this option if you want a VMware sensor to reuse a single session for multiple sensor scans to query data. With this option, the sensor does not need to log in and out for each sensor scan. We recommend that you use this option because it reduces network load and log entries on the target device. This can increase performance. ▪ Create a new session for each scan: If you select this option, PRTG does not reuse a session and a VMware sensor has to log in and out for each sensor scan. This can decrease performance.

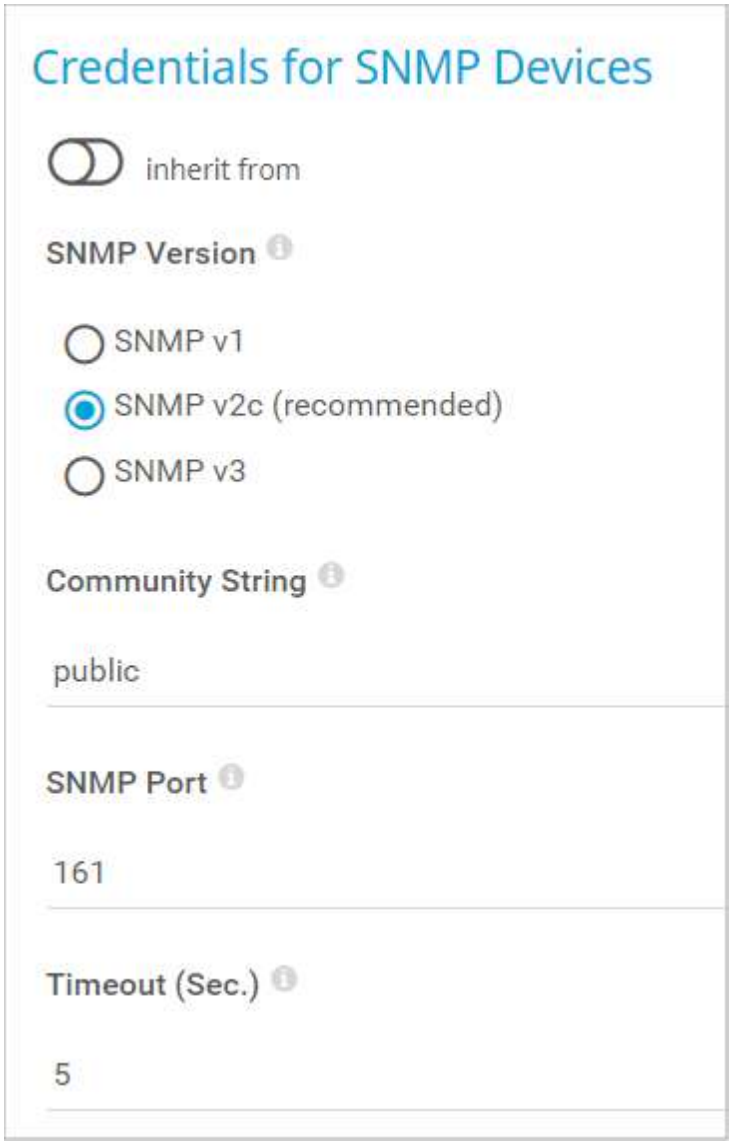
Credentials for SNMP Devices

Click to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Cisco IP SLA
- SNMP APC Hardware
- SNMP Buffalo TS System Health
- SNMP Cisco ADSL
- SNMP Cisco ASA VPN Connections
- SNMP Cisco ASA VPN Traffic
- SNMP Fujitsu System Health v2
- SNMP Hardware Status
- SNMP HP LaserJet Hardware
- SNMP HPE BladeSystem Blade
- SNMP HPE BladeSystem Enclosure System Health
- SNMP HPE ProLiant Logical Disk
- SNMP NetApp Enclosure
- SNMP NetApp I/O
- SNMP NetApp License
- SNMP NetApp Logical Unit
- SNMP NetApp Network Interface
- SNMP NetApp System Health
- SNMP Nutanix Cluster Health

- SNMP Cisco ASA VPN Users
- SNMP Cisco CBQoS
- SNMP Cisco System Health
- SNMP Cisco UCS Blade
- SNMP Cisco UCS Chassis
- SNMP Cisco UCS Physical Disk
- SNMP Cisco UCS System Health
- SNMP CPU Load
- SNMP Custom
- SNMP Custom Advanced
- SNMP Custom String
- SNMP Custom String Lookup
- SNMP Custom Table
- SNMP Dell EqualLogic Logical Disk
- SNMP Dell EqualLogic Member Health
- SNMP Dell EqualLogic Physical Disk
- SNMP Dell Hardware
- SNMP Dell PowerEdge Physical Disk
- SNMP Dell PowerEdge System Health
- SNMP Disk Free
- SNMP HPE ProLiant Memory Controller
- SNMP HPE ProLiant Network Interface
- SNMP HPE ProLiant Physical Disk
- SNMP HPE ProLiant System Health
- SNMP IBM System X Logical Disk
- SNMP IBM System X Physical Disk
- SNMP IBM System X Physical Memory
- SNMP IBM System X System Health
- SNMP interSeptor Pro Environment
- SNMP Juniper NS System Health
- SNMP LenovoEMC Physical Disk
- SNMP LenovoEMC System Health
- SNMP Library
- SNMP Linux Disk Free
- SNMP Linux Load Average
- SNMP Linux Meminfo
- SNMP Linux Physical Disk
- SNMP Memory
- SNMP NetApp Disk Free
- SNMP Nutanix Hypervisor
- SNMP Poseidon Environment
- SNMP Printer
- SNMP QNAP Logical Disk
- SNMP QNAP Physical Disk
- SNMP QNAP System Health
- SNMP Rittal CMC III Hardware Status
- SNMP RMON
- SNMP SonicWall System Health
- SNMP SonicWall VPN Traffic
- SNMP Synology Logical Disk
- SNMP Synology Physical Disk
- SNMP Synology System Health
- SNMP System Uptime
- SNMP Traffic
- SNMP Trap Receiver
- SNMP Windows Service



Credentials for SNMP Devices

Setting	Description
SNMP Version	Select the Simple Network Management Protocol (SNMP) version for the connection to the target SNMP device: ▪ SNMP v1: Use SNMP v1 for the connection. SNMP v1 only offers clear-text data transmission. ⓘ SNMP v1 does not support 64-bit counters. This might result in invalid data when you monitor traffic via SNMP. ▪ SNMP v2c (recommended): Use SNMP v2c for the connection. SNMP v2c also only offers clear-text data transmission but it supports 64-bit counters.

Setting	Description
	▪ SNMP v3: Use SNMP v3 for the connection. SNMP v3 provides secure authentication and data encryption. ⓘ SNMP v3 has performance limitations because of the use of encryption. The main limiting factor is CPU power. Also keep in mind that SNMP v3, unlike SNMP v1 and v2c, does not scale with more CPU power. Because of this limitation, PRTG can only handle a limited number of requests per second so that you can use only a limited number of sensors using SNMP v3. If you see an increase in Interval Delay or Open Requests with the Probe Health sensor, distribute the load over multiple probes 3621. SNMP v1 and SNMP v2c do not have this limitation.
Community String	This setting is only visible if you select SNMP v1 or SNMP v2c (recommended) above. Enter the community string of your device. This is like a clear-text password for simple authentication. ⓘ We recommend that you use the default value.
Authentication Method	This setting is only visible if you select SNMP v3 above. Select the authentication method: ▪ MD5: Use message-digest algorithm 5 (MD5) for authentication. ▪ SHA: Use Secure Hash Algorithm (SHA) for authentication. ▪ SHA-224: Use SHA-224 for authentication. ▪ SHA-256: Use SHA-256 for authentication. ▪ SHA-384: Use SHA-384 for authentication. ▪ SHA-512: Use SHA-512 for authentication. ⓘ If you do not want to use authentication but you need SNMP v3, for example, because your device requires context, you can leave the Password field empty. In this case, PRTG uses SNMP_SEC_LEVEL_NOAUTH and it entirely deactivates authentication. ⓘ The authentication method you select must match the authentication method of your device.
User Name	This setting is only visible if you select SNMP v3 above. Enter the user name for access to the target SNMP device. ⓘ The user name that you enter must match the user name of your device.
Password	This setting is only visible if you select SNMP v3 above. Enter the password for access to the target SNMP device. ⓘ The password that you enter must match the password of your device.

Setting	Description
Encryption Type	This setting is only visible if you select SNMP v3 above. Select an encryption type: ▪ DES: Use Data Encryption Standard (DES) as the encryption algorithm. ▪ AES: Use Advanced Encryption Standard (AES) as the encryption algorithm. ▪ AES-192: Use AES-192 as the encryption algorithm. ▪ AES-256: Use AES-256 as the encryption algorithm. ⓘ The encryption type that you select must match the encryption type of your device.
Encryption Key	This setting is only visible if you select SNMP v3 above. Enter an encryption key. If you provide a key, PRTG encrypts SNMP data packets with the encryption algorithm that you selected above. Enter a string or leave the field empty. ⓘ The encryption key that you enter must match the encryption key of your device. If the encryption keys do not match, you do not get an error message.
Context Name	This setting is only visible if you select SNMP v3 above. Enter a context name only if the configuration of the device requires it. Context is a collection of management information that is accessible by an SNMP device. Enter a string.
SNMP Port	Enter the port for the connection to the SNMP target device. Enter an integer. The default port is 161. ⓘ We recommend that you use the default value.
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

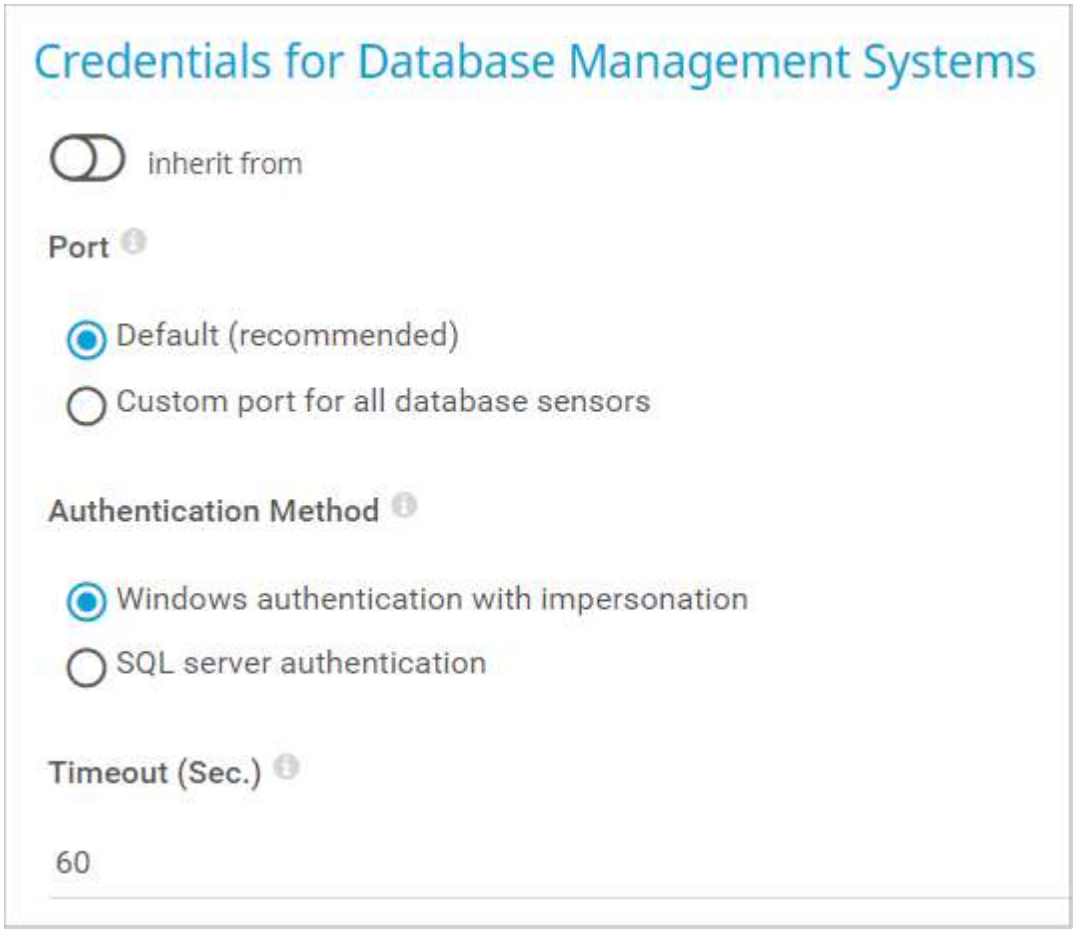
Credentials for Database Management Systems

Click to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- ADO SQL v2
- Microsoft SQL v2
- MySQL v2
- Oracle SQL v2

- PostgreSQL



Credentials for Database Management Systems

Setting	Description
Port	Enter a custom port for database connections. Enter an integer. ⓘ PRTG uses this custom port for all database sensors and for connections to all your databases.
Custom Port	Select the authentication method for the connection to the Structured Query Language (SQL) database: ▪ Windows authentication with impersonation: PRTG uses the Windows credentials that you define in settings that are higher in the object hierarchy 131, for example, in the settings of the parent device; for the database connection. ⓘ The user whose credentials PRTG uses needs to have permission to log in to the probe system with a database sensor. This is necessary for the impersonation. ▪ SQL server authentication: Use explicit credentials for database connections. Enter a user name and password below.

Setting	Description
Authentication Method	This setting is only visible if you select SQL server authentication above. Enter the user name for the database connection.
User Name	This setting is only visible if you select SQL server authentication above. Enter the password for the database connection.
Password	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).

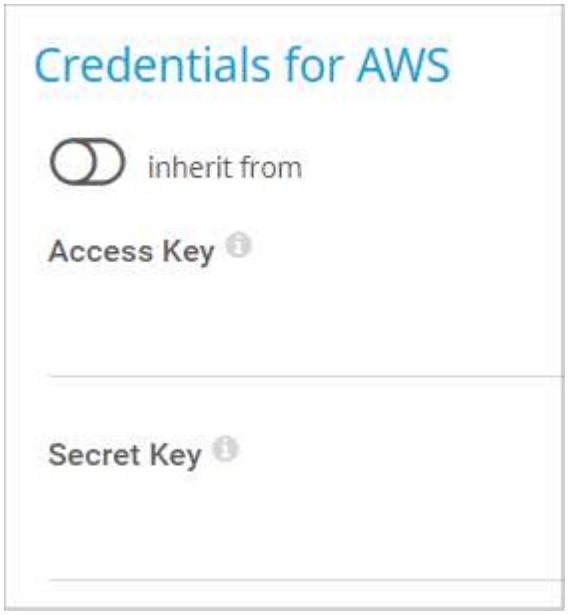
Credentials for AWS

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- AWS Alarm v2
- AWS Cost
- AWS EBS v2
- AWS EC2 v2
- AWS ELB v2
- AWS RDS v2

For more information about the permissions that are necessary to query the AWS API, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?



Credentials for AWS

Setting	Description
Access Key	Enter the Amazon Web Services (AWS) access key.
Secret Key	Enter the AWS secret key.

Credentials for Microsoft 365

Click to interrupt the inheritance 135.

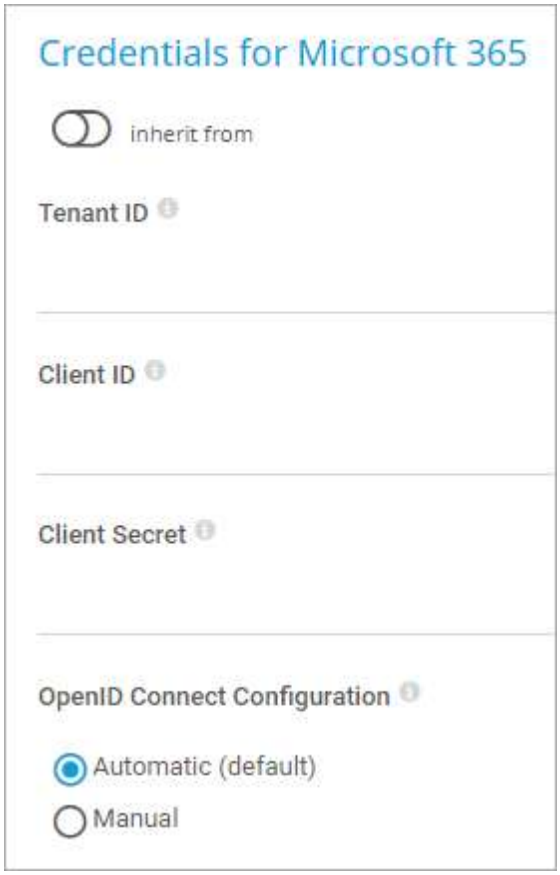
The settings you define in this section apply to the following sensors:

- Microsoft 365 Mailbox
- Microsoft 365 Service Status
- Microsoft 365 Service Status Advanced

The sensors use the credentials to authenticate with Azure Active Directory (Azure AD).

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Service Status sensor and the Microsoft 365 Service Status Advanced sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

For more information about the credentials and the permissions that are necessary to use the Microsoft 365 Mailbox sensor, see the Knowledge Base: How do I obtain credentials and set permissions for the Microsoft 365 Mailbox sensor?



Credentials for Microsoft 365

Setting	Description
Tenant ID	Enter the Azure AD tenant ID. A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Azure AD client ID.
Client Secret	Enter the Azure AD client secret.
OpenID Connect Configuration	Select if you want to manually enter the authorization endpoint URL and token endpoint URL that PRTG uses to access Microsoft Graph. Choose between: ▪ Automatic (default): PRTG automatically determines the authorization endpoint URL and the token endpoint URL. ▪ Manual: Manually enter the authorization endpoint URL and the token endpoint URL.
Authorization Endpoint	Enter the authorization endpoint URL including the server. Authorization endpoint URL example:

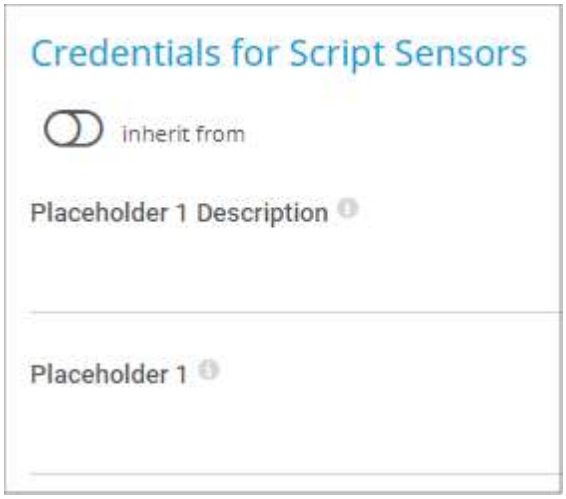
Setting	Description
	`https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/authorize` Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.
Token Endpoint	Enter the token endpoint URL including the server. Token endpoint URL example: `https://login.microsoftonline.com/<tenant-ID>/oauth2/v2.0/token` Make sure to replace <tenant-ID> with the directory (tenant) ID from Azure AD.

Credentials for Script Sensors

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- EXE/Script
- EXE/Script Advanced
- Python Script Advanced
- SSH Script
- SSH Script Advanced



Credentials for Script Sensors

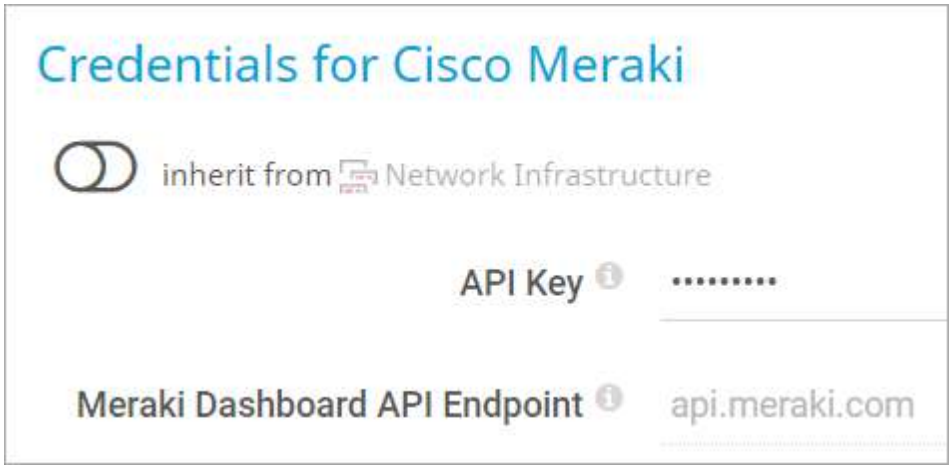
Setting	Description
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder1 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder2 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder3 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder4 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the script execution if you add %scriptplaceholder5 in the argument list. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Cisco Meraki

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Cisco Meraki License
- Cisco Meraki Network Health



Credentials for Cisco Meraki

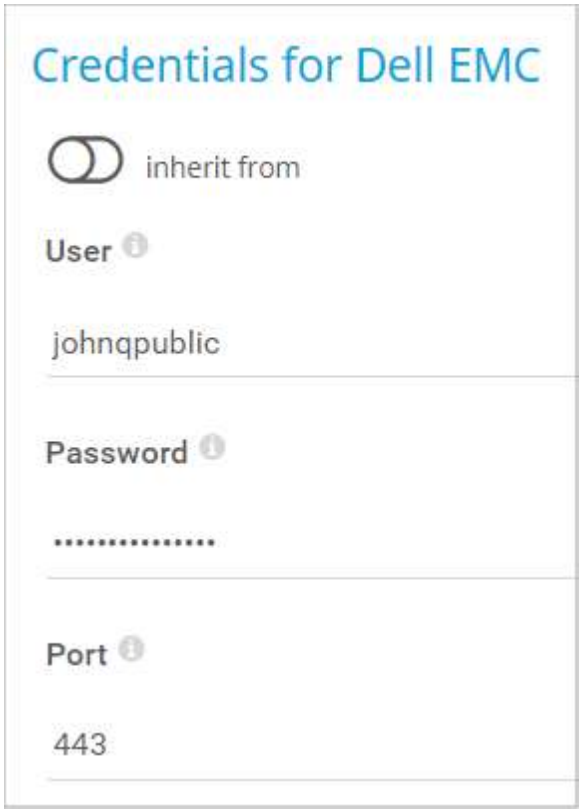
Setting	Description
API Key	Enter an API key that the sensor uses for authentication against the Cisco Meraki Dashboard API.
Meraki Dashboard API Endpoint	Enter the endpoint for the Cisco Meraki Dashboard API. The default api.meraki.com should be valid for most use cases. ⓘ See the Cisco Meraki Dashboard API documentation for other possible choices.

Credentials for Dell EMC

Click to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- Dell EMC Unity Enclosure Health v2
- Dell EMC Unity File System v2
- Dell EMC Unity Storage Capacity v2
- Dell EMC Unity Storage LUN v2
- Dell EMC Unity Storage Pool v2
- Dell EMC Unity VMware Datastore v2



Credentials for Dell EMC

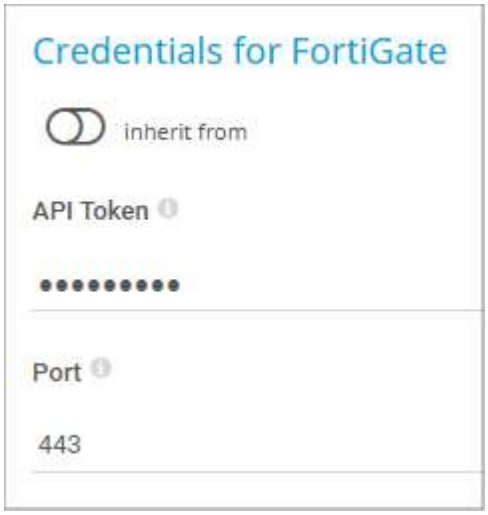
Setting	Description
User Name	Enter the user name for access to the Dell EMC system.
Password	Enter the password for access to the Dell EMC system.
Port	Enter the port for the connection to the Dell EMC system. The default port for secure connections is 443.

Credentials for FortiGate

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- FortiGate System Statistics
- FortiGate VPN Overview



Credentials for FortiGate

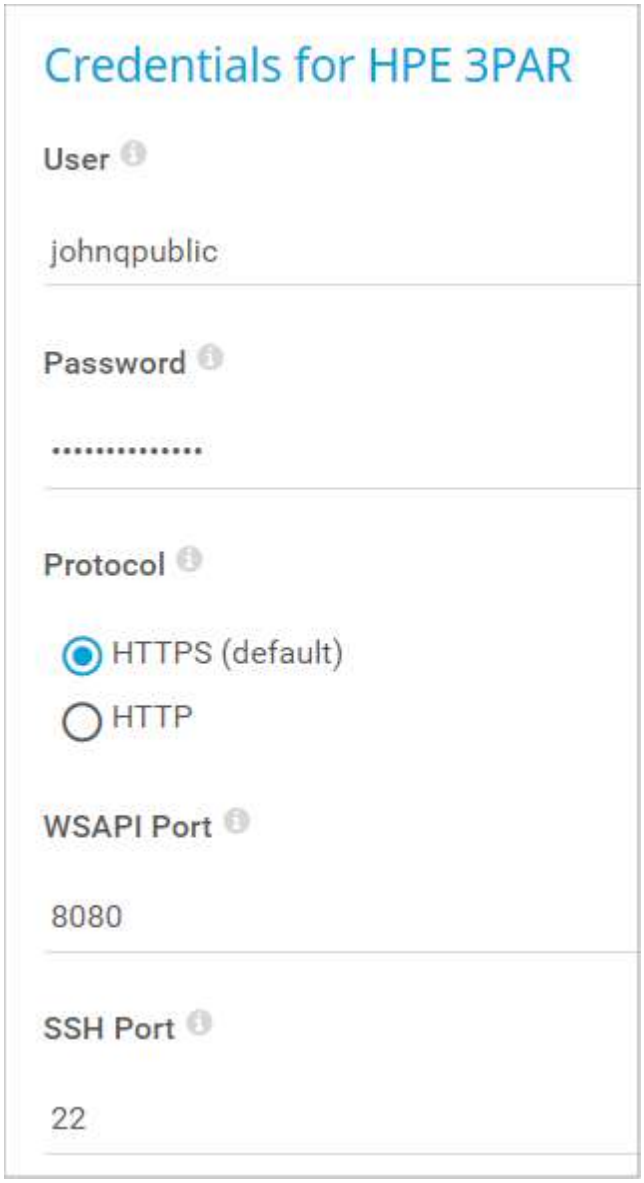
Setting	Description
API Token	Enter the API token for access to the FortiGate system.
Port	Enter the port for the connection to the FortiGate system. The default port for secure connections is 443.

Credentials for HPE 3PAR

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- HPE 3PAR Common Provisioning Group
- HPE 3PAR Drive Enclosure
- HPE 3PAR Virtual Volume



Credentials for HPE 3PAR

Setting	Description
User Name	Enter the user name for access to the HPE 3PAR system.
Password	Enter the password for access to the HPE 3PAR system.
Protocol	Select the protocol that you want to use for the connection to the HPE 3PAR system: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Setting	Description
WSAPI Port	Enter the Web Services API (WSAPI) port for the connection to the HPE 3PAR system. The default port for secure connections is 8080 and the default port for unsecure connections is 8008. For more information, see the Knowledge Base: Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?
SSH Port	Enter the SSH port for the connection to the HPE 3PAR system. The default port for secure connections is 22.

Credentials for HTTP

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensor:

- HTTP v2

Credentials for HTTP

Setting	Description
Authentication Method	Select the authentication method for access to the server. Choose between: ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the server.

Setting	Description
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the server.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the server.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder1 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder2 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder3 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder4 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the HTTP request if you add %httpplaceholder5 in the URL, POST Body, and Custom Header fields of the HTTP v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Microsoft Azure

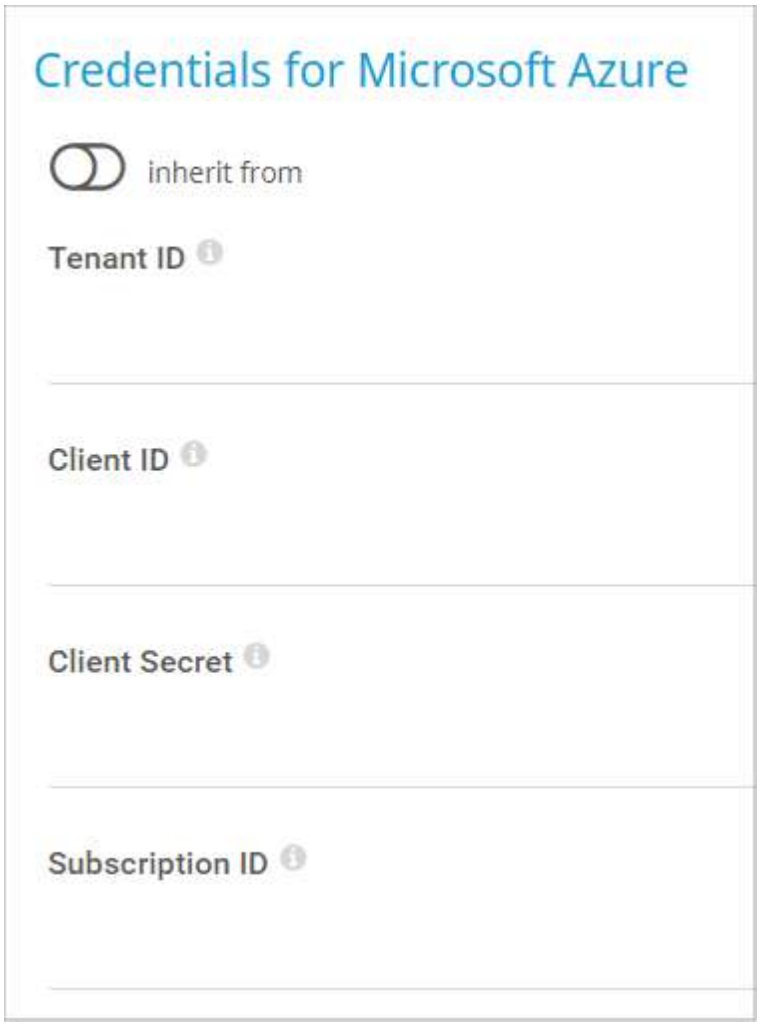
Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Microsoft Azure SQL Database
- Microsoft Azure Storage Account
- Microsoft Azure Subscription Cost
- Microsoft Azure Virtual Machine

The sensors use the credentials to authenticate with Azure Active Directory (Azure AD).

For more information about the credentials and permissions that are necessary use the Microsoft Azure sensors, see the Knowledge Base: How do I obtain credentials and create custom roles for the Microsoft Azure sensors?



Credentials for Microsoft Azure

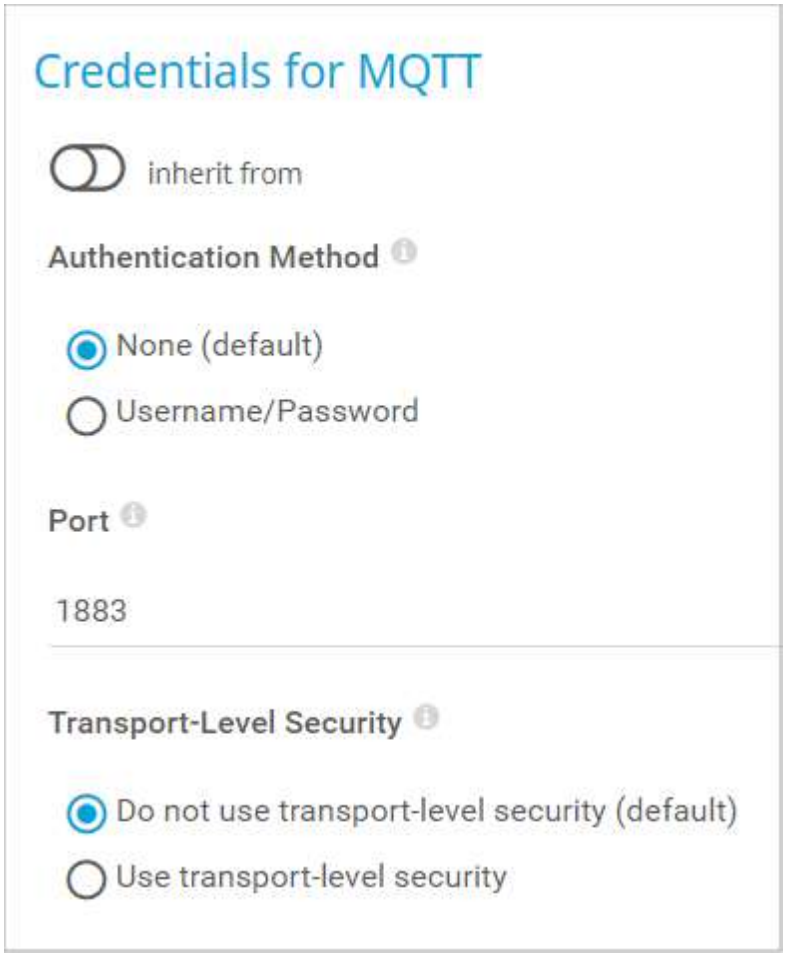
Setting	Description
Tenant ID	Enter the Azure AD tenant ID. A tenant ID must be a 32-digit sequence in hexadecimal notation.
Client ID	Enter the Azure AD client ID.
Client Secret	Enter the Azure AD client secret.
Subscription ID	Enter the Azure AD subscription ID.

Credentials for MQTT

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- MQTT Round Trip
- MQTT Statistics
- MQTT Subscribe Custom



Credentials for MQTT

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the MQTT broker. ▪ None (default): Connect without credentials. ▪ User name and password: Define credentials for the connection.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Message Queue Telemetry Transport (MQTT) broker.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the MQTT broker.
Port	Enter the port for the connection to the MQTT broker. The default port for secure connections is 8883 and the default port for unsecure connections is 1883.

Setting	Description
Transport-Level Security	Select if you want to use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection: ▪ Do not use transport-level security: Establish the connection without connection security. ▪ Use transport-level security: Establish the connection with the strongest SSL/TLS method that the target device provides.
Server Authentication	This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for server authentication. ▪ Disable (default): Do not use a certificate for server authentication. ▪ Enable: Use a certificate for server authentication.
CA Certificate	This setting is only visible if you enable Server Authentication above. Paste the certificate authority (CA) certificate for the verification of the MQTT broker. ⓘ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Authentication	This setting is only visible if you select Use transport-level security above. Select if you want to use a certificate for client authentication. ▪ Disable (default): Do not use a certificate for client authentication. ▪ Enable: Use a certificate for client authentication.
Client Certificate	This setting is only visible if you enable Client Authentication above. Paste the certificate that you created for authenticating the sensor against the MQTT broker. ⓘ The certificate must be in PEM format.
Client Key	This setting is only visible if you enable Client Authentication above. Enter the client key for access to the MQTT broker. ⓘ The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you enable Client Authentication above. Enter the password for the client key.

Credentials for NetApp

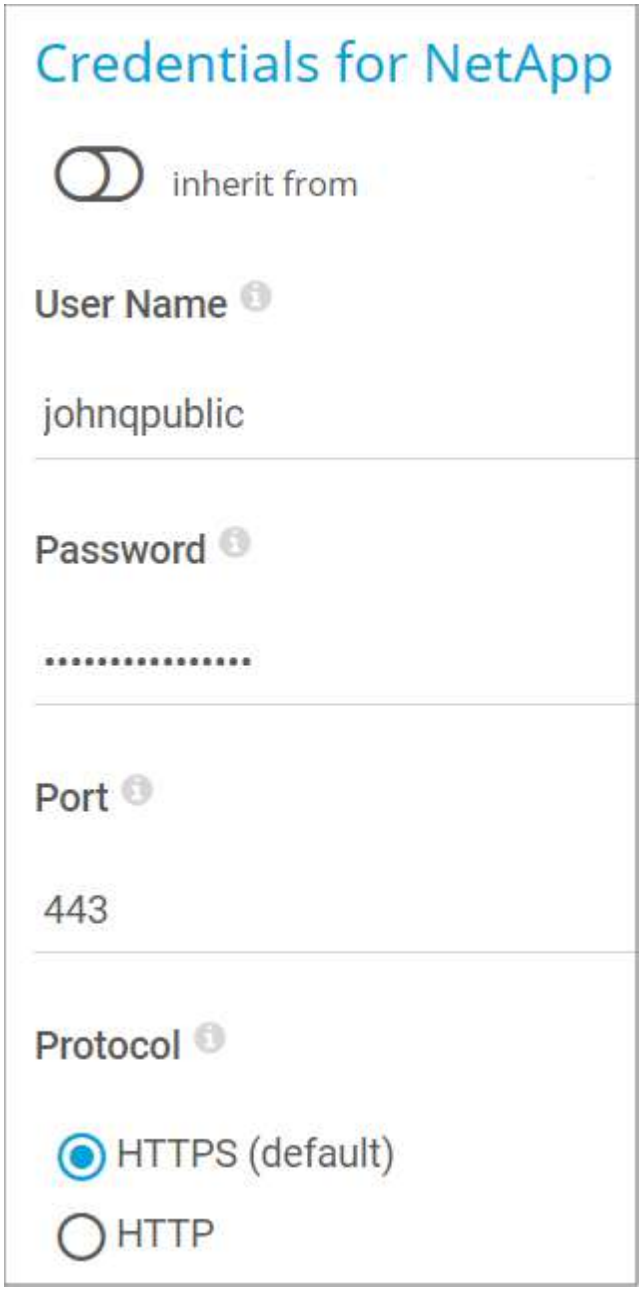
Click to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensors:

- NetApp Aggregate v2

- NetApp I/O v2
- NetApp LIF v2
- NetApp LUN v2
- NetApp NIC v2
- NetApp Physical Disk v2
- NetApp SnapMirror v2
- NetApp System Health v2
- NetApp Volume v2

The sensors use the credentials for access to the ONTAP System Manager.



Credentials for NetApp

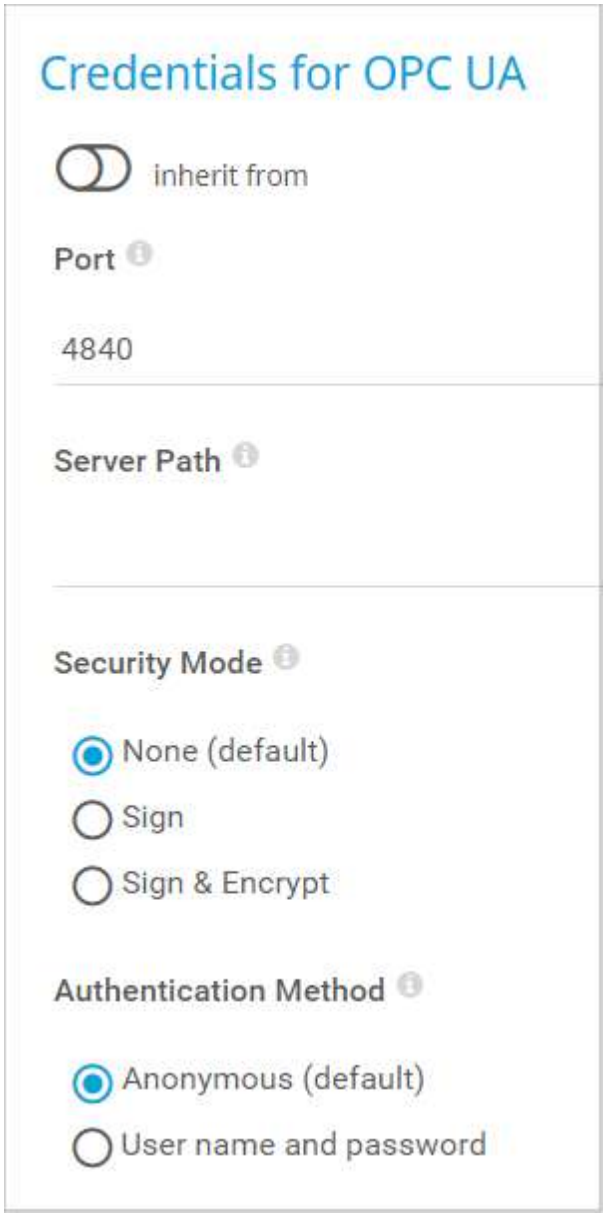
Setting	Description
User Name	Enter a user name for access to the ONTAP System Manager.
Password	Enter the password for access to the ONTAP System Manager.
Port	Enter the port for the connection to the ONTAP System Manager. The default port for secure connections is 443.
Protocol	Select the protocol that you want to use for the connection to the ONTAP System Manager. Choose between: ▪ HTTPS (default) ▪ HTTP

Credentials for OPC UA

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Beckhoff IPC System Health
- OPC UA Certificate
- OPC UA Custom
- OPC UA Server Status



Credentials for OPC UA

Setting	Description
Port	Enter the port for the connection to the OPC Unified Architecture (OPC UA) server. The default port for secure connections is 4840.
Server Path	Enter the path of the OPC UA server endpoint if you run more than one server under the same IP address or DNS name.
Security Mode	Select if you want to use encryption: ▪ None (default): Do not use encryption. ▪ Sign: Sign messages between the sensor and the OPC UA server.

Setting	Description
	▪ Sign & Encrypt: Sign and encrypt messages between the sensor and the OPC UA server.
Security Policy	This setting is only visible if you select Sign or Sign & Encrypt above. Select if you want to use a security policy and define which policy you want to use: ▪ None (default): Do not use a security policy. ▪ Basic256Sha256: Use the Basic256Sha256 security policy. ▪ Basic256: Use the Basic256 security policy.
Client Certificate	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the certificate that you created for authenticating the sensor against the OPC UA server. ⓘ The certificate must meet the following requirements: ▪ The key size must be 2048-bit. ▪ The secure hash algorithm must be SHA256. ▪ DataEncipherment must be part of the KeyUsage certificate extension. ▪ A uniform resource indicator (URI) must be set in subjectAltName. ▪ The certificate must be in Privacy-Enhanced Mail (PEM) format.
Client Key	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the client key for access to the OPC UA server. ⓘ The client key must be in PEM format and it must be encrypted using the Client Key Password.
Client Key Password	This setting is only visible if you select Sign or Sign & Encrypt above. Enter the password for the client key.
Authentication Method	Select if you want to connect without credentials or define credentials for access to the OPC UA server: ▪ Anonymous (default): Connect without credentials. ▪ User name and password: Define credentials for the connection. ⓘ Most OPC UA servers do not support User name and password authentication without a client certificate. To use User name and password authentication, select Sign or Sign & Encrypt under Security Mode and Basic256Sha256 or Basic256 under Security Policy and enter the Client Certificate, Client Key, and Client Key Password that you want to use.

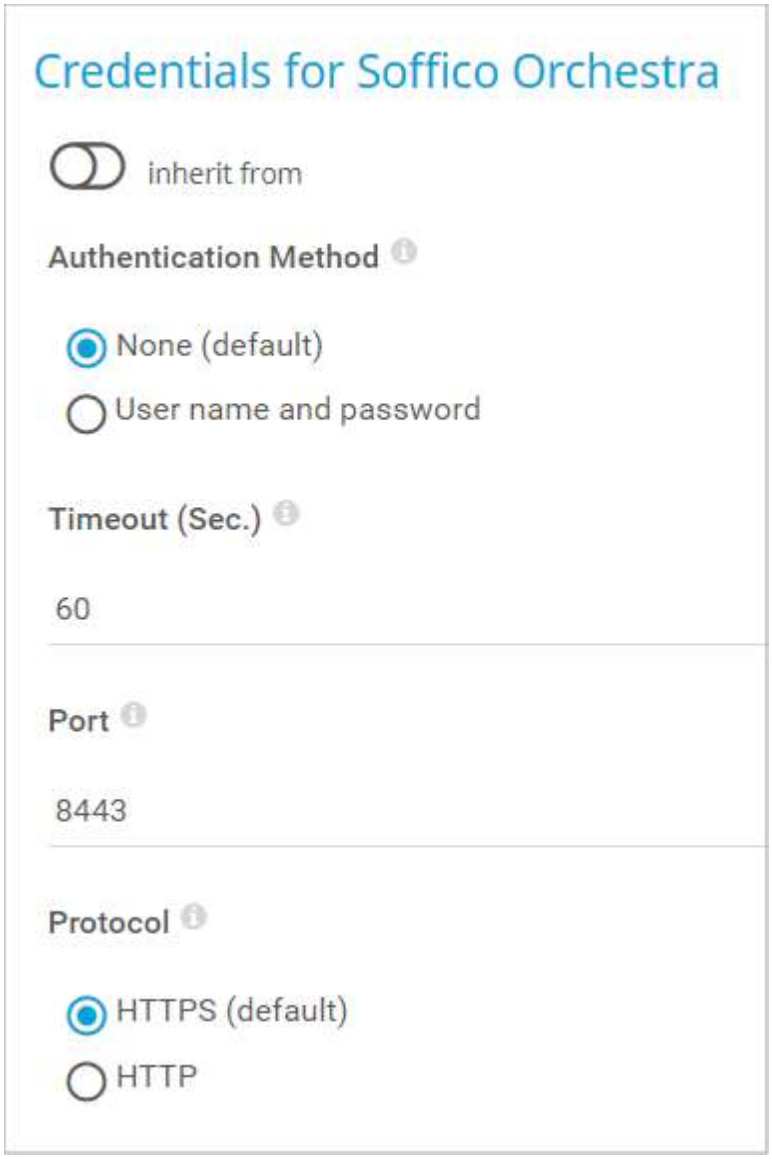
Setting	Description
	If you select None (default) under Security Mode and use User name and password authentication, PRTG sends the unencrypted password to the OPC UA server.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the OPC UA server.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the OPC UA server.

Credentials for Soffico Orchestra

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensor:

- Soffico Orchestra Channel Health



Credentials for Soffico Orchestra

Setting	Description
Authentication Method	Select if you want to connect without credentials or define credentials for access to the Orchestra platform: ▪ None (default): Connect without credentials. ▪ User name and password: Define credentials for the connection.
User Name	This setting is only visible if you select User name and password above. Enter the user name for access to the Orchestra platform.
Password	This setting is only visible if you select User name and password above. Enter the password for access to the Orchestra platform.

Setting	Description
Timeout (Sec.)	Enter a timeout in seconds for the request. Enter an integer. The maximum timeout value is 300 seconds (5 minutes).
Port	Enter the port for the connection to the Orchestra platform. The default port for secure connections is 8443 and the default port for unsecure connections is 8019.
Protocol	Select the protocol that you want to use for the connection to the Orchestra platform: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.

Credentials for Redfish

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Redfish Power Supply
- Redfish System Health
- Redfish Virtual Disk

Credentials for Redfish

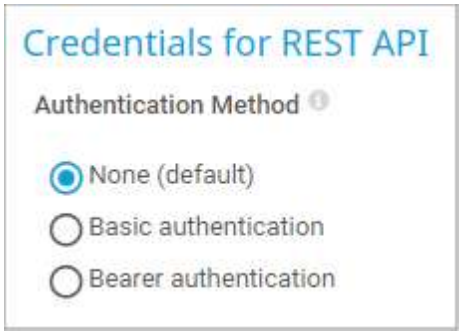
Setting	Description
User Name	Enter the user name for access to the Redfish system.
Password	Enter the password for access to the Redfish system.
Protocol	Select the protocol that you want to use for the connection to the Redfish system. Choose between: ▪ HTTPS (default): Use a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) secured connection. ▪ HTTP: Use an unsecure connection.
Port	Enter the port for the connection to the Redfish system. The default port for secure connections is 443.

Credentials for REST API

Click to interrupt the inheritance 135.

ⓘ The settings you define in this section apply to the following sensor:

- REST Custom v2



Credentials for REST API

Setting	Description
Authentication Method	Select the authentication method for access to the Representational State Transfer (REST) application programming interface (API): ▪ None (default): Use no authentication. ▪ Basic authentication: Use basic authentication. ▪ Bearer authentication: Use an OAuth2 bearer token.
User Name	This setting is only visible if you select Basic authentication above. Enter the user name for access to the REST API.
Password	This setting is only visible if you select Basic authentication above. Enter the password for access to the REST API.
Bearer Token	This setting is only visible if you select Bearer authentication above. Enter a bearer token for access to the REST API.
Placeholder 1 Description	Enter a description for Placeholder 1, for example information about the purpose or content of the placeholder.
Placeholder 1	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder1 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 2 Description	Enter a description for Placeholder 2, for example information about the purpose or content of the placeholder.
Placeholder 2	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder2 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

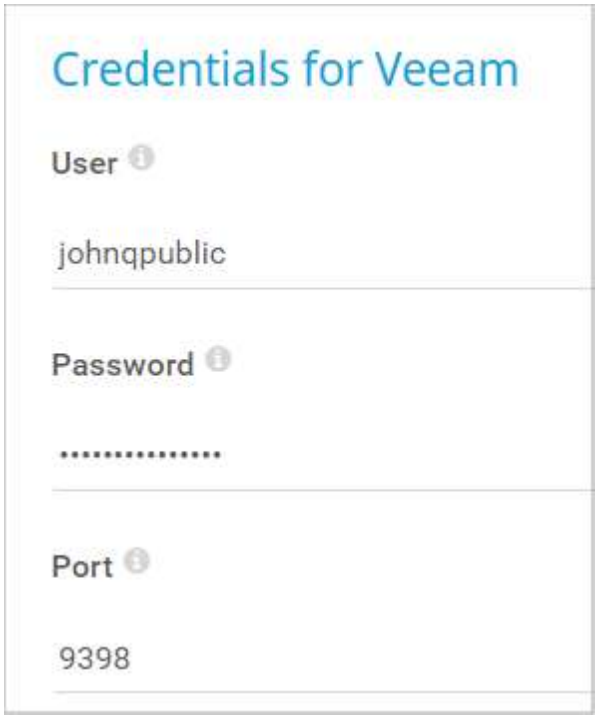
Setting	Description
Placeholder 3 Description	Enter a description for Placeholder 3, for example information about the purpose or content of the placeholder.
Placeholder 3	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder3 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 4 Description	Enter a description for Placeholder 4, for example information about the purpose or content of the placeholder.
Placeholder 4	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder4 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.
Placeholder 5 Description	Enter a description for Placeholder 5, for example information about the purpose or content of the placeholder.
Placeholder 5	Enter a value for the placeholder. PRTG inserts the value for the REST API request if you add %restplaceholder5 in the Request URL, POST Body, and Custom Headers fields of the REST Custom v2 sensor. PRTG does not display the value in the sensor log or the sensor's settings.

Credentials for Veeam

Click to interrupt the inheritance 135.

The settings you define in this section apply to the following sensors:

- Veeam Backup Job Status
- Veeam Backup Job Status Advanced



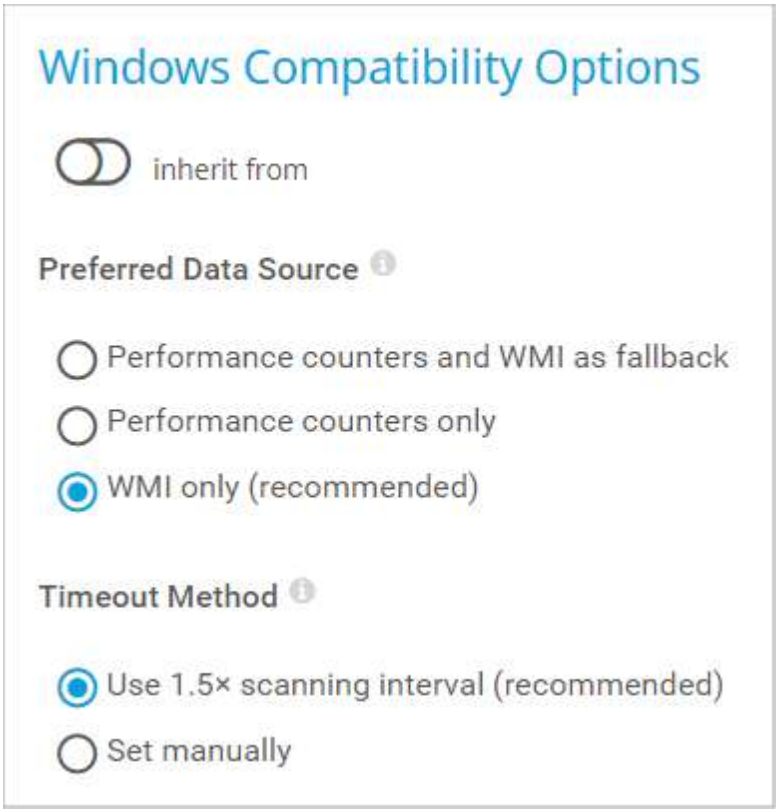
Credentials for Veeam

Setting	Description
User Name	Enter the user name for access to the Veeam Backup Enterprise Manager.
Password	Enter the password for access to the Veeam Backup Enterprise Manager.
Port	Enter the port for the connection to the Veeam Backup Enterprise Manager. The default port for secure connections is 9398.

Windows Compatibility Options

Click to interrupt the inheritance 135.

If you experience problems when you monitor via Windows sensors, use the following compatibility options for troubleshooting.



Windows Compatibility Options

Setting	Description
Preferred Data Source	ⓘ This setting only applies to hybrid sensors that use both performance counters and Windows Management Instrumentation (WMI). The setting does not apply to other sensors. Define the method that Windows sensors use to query data: ▪ Performance counters and WMI as fallback: Try to query data via performance counters. If this is not possible, establish a connection via WMI. ▪ Performance counters only: Query data via performance counters only. If this is not possible, the sensor returns no data. ▪ WMI only (recommended): Query data via WMI only. If this is not possible, the sensor returns no data. We recommend that you use this option.
Timeout Method	Select the time that the sensor waits for the return of the WMI query before the sensor cancels the query and shows an error message: ▪ Use 1.5× scanning interval (recommended): Multiply the scanning interval of the sensor by 1.5 and use the resulting value. ▪ Set manually: Manually enter a timeout value.

Setting	Description
	ⓘ We recommend that you use the default value. ⓘ If you experience ongoing timeout errors, try increasing the timeout value.
Timeout (Sec.)	This setting is only visible if you select Set manually above. Enter the time the sensor waits for the return of its WMI query before it cancels it and shows an error message. Enter an integer. The maximum timeout value is 900 seconds (15 minutes).

SNMP Compatibility Options

Click to interrupt the inheritance 135.

If you experience problems when you monitor via Simple Network Management Protocol (SNMP) sensors, use the following compatibility options for troubleshooting.

SNMP Compatibility Options

inherit from

SNMP Delay (ms)

0

Failed Requests

- (•) Retry (recommended)
- ( ) Do not retry

Overflow Values

- ( ) Ignore overflow values
- (•) Handle overflow values as valid results

Zero Values

- (•) Ignore zero values for delta sensors (recommended)
- ( ) Handle zero values as valid results for delta sensors

32-bit/64-bit Counters

- (•) Use 64-bit counters if available (recommended)
- ( ) Use 32-bit counters only

Request Mode

- (•) Use multi get (recommended)
- ( ) Use single get

Walk Mode

- (•) Use GETBULK requests (recommended)
- ( ) Use GETNEXT requests

Setting	Description
SNMP Delay (ms)	Enter the time in milliseconds (ms) that PRTG waits between two SNMP requests. This can increase device compatibility. Enter an integer. You can define a delay between 0 and 100. PRTG does not support higher delays. ⓘ We recommend that you use the default value. ⓘ If you experience SNMP connection failures, try increasing the delay.
Failed Requests	Select if an SNMP sensor tries again after a request fails: ▪ Retry (recommended): Try again if an SNMP request fails. This can prevent false error messages because of temporary timeout failures. ▪ Do not retry: Do not retry if an SNMP request fails. If you select this option, an SNMP sensor shows a Down status earlier.
Overflow Values	Select how PRTG handles overflow values. Some devices do not correctly handle internal buffer overflows. This can cause false peaks. ▪ Ignore (default): Ignore overflow values and do not include them in the monitoring data. We recommend that you use this option. ▪ Handle overflow values as valid results: Regard all overflow values as regular data and include them in the monitoring data. ⓘ If you experience problems because of strange peaks in your data graphs, change this option. Peaks might indicate that the target device resets counters without an overflow. PRTG interprets such behavior as overflow that results in data peaks. Select the option Ignore (default) in this case. For more details, see the Knowledge Base: What is the Overflow Values setting in the SNMP Compatibility Options?
Zero Values	Select how PRTG handles zero values. Some devices send incorrect zero values. This can cause false peaks. ▪ Ignore (recommended): Ignore zero values and do not include them in the monitoring data. We recommend that you use this option. ⓘ If you experience problems, try changing this option. ▪ Handle zero values as valid results for delta sensors: Regard all zero values as regular data and include them in the monitoring data.
32-bit/64-bit Counters	Select the type of traffic counters that PRTG searches for on a device: ▪ Use 64-bit counters if available (recommended): The interface scan uses 64-bit traffic counters, if available. This can avoid buffer overflows in the devices ⓘ We recommend that you use the default value. ⓘ If you experience problems, try changing this option.

Setting	Description
	▪ Use 32-bit counters only: The interface scan always uses 32-bit traffic counters, even if 64-bit counters are available. This can make monitoring more reliable for some devices.
Request Mode	Select the request method that PRTG uses for SNMP sensors: ▪ Use multi get (recommended): Bundle multiple SNMP requests into one request. We recommend that you use this option. ⓘ If you experience problems, try changing this option. ▪ Use single get: Use one request for each SNMP value. This can increase compatibility with older devices. ⓘ PRTG uses paging for SNMP requests. This means that if a sensor has to query more than 20 object identifiers (OID), it automatically polls the OIDs in packages of 20 OIDs each.
Walk Mode	Select the kind of SNMP walk that PRTG uses for SNMP sensors: ▪ Use GETBULK requests (recommended): Request the next x OIDs in one SNMP request. The default value is 10. It is dynamic based on the response size. ⓘ This option only works with devices that support SNMP as of version v2c. Make sure that you set the correct SNMP Version in the Credentials for SNMP Devices settings of the parent device or inherit it from objects that are higher in the object hierarchy 131. ▪ Use GETNEXT requests: Request one OID at a time. This can increase compatibility with older devices or with devices that have insufficient SNMP BULKWALK support.
Port Name Template	Select how PRTG displays the name of SNMP sensors. Enter a template that uses several variables. When you add new sensors, PRTG scans the interface for available counters at certain OIDs. At each OID, several fields with interface descriptions are usually available. They are different for every device and OID. PRTG uses the information in these fields to name the sensors. If a field is empty or if it is not available, PRTG adds an empty string to the name. By default, the port name template is ([port]) [ifalias] [ifsensor], which creates a name like (001) Ethernet1 Traffic. You can use and combine any field names that are available at an OID of your device, for example: ▪ [port]: The port number of the monitored interface. ▪ [ifalias]: The 'alias' name for the monitored interface as specified by a network manager, providing a non-volatile handling. ▪ [ifname]: The textual name of the monitored interface as assigned by the local device. ▪ [ifdescr]: A textual string containing information about the target device or interface, for example, manufacturer, product name, or version.

Setting	Description
	▪ [ifspeed]: An estimate of the monitored interface's current bandwidth (Kbit/s). ▪ [ifsensor]: The type of the sensor, this is Traffic or RMON. This helps to differentiate between SNMP Traffic and SNMP RMON sensors. For more information about SNMP sensor names, see the Knowledge Base: How can I change the defaults for names automatically generated for new SNMP sensors?
Port Name Update	Select how PRTG reacts if you change the names of ports in your physical device (for example, a switch or router): ▪ Keep port names (use this if you edit the names in PRTG): Do not automatically adjust sensor names. This is the best option if you want to manually change names in PRTG. ▪ Automatically update sensor names if port names change in the device: If PRTG detects port name changes in your physical device, it tries to automatically adjust the sensor names accordingly. For more information about automatic name updates, see the Knowledge Base: Automatically update port name and number for SNMP Traffic sensors when the device changes them.
Port Identification	Select the field that PRTG uses for SNMP interface identification: ▪ Automatic identification (recommended): Try the ifAlias field first to identify an SNMP interface and then try ifDescr. ⓘ PRTG does not automatically try ifName. ▪ Use ifAlias: For most devices, ifAlias is the best field to use for unique interface names. ▪ Use ifDescr: Use this option if the port order of your device changes after a restart, and if no ifAlias field is available. For example, this is the best option for Cisco ASA devices. ⓘ If you use this option, it is important that your device returns unique interface names in the ifDescr field. ▪ Use ifName: You can also use this option if no unique ifAlias is available. ⓘ If you use this option, it is important that your device returns unique interface names in the ifName field. ▪ Do not update ports: Use this option to disable the automatic port identification.
Start Interface Index	ⓘ This setting only applies to SNMP Traffic sensors and to Cisco IP SLA sensors. Enter the index at which PRTG starts to query the interface range during sensor creation. Enter 0 for the automatic mode.

Setting	Description
	ⓘ We recommend that you use the default value.
End Interface Index	ⓘ This setting only applies to SNMP Traffic sensors and to Cisco IP SLA sensors. Enter the index at which PRTG stops querying the interface range during sensor creation. Enter 0 for the automatic mode. ⓘ We recommend that you use the default value.

Proxy Settings for HTTP Sensors

Click to interrupt the inheritance 135.

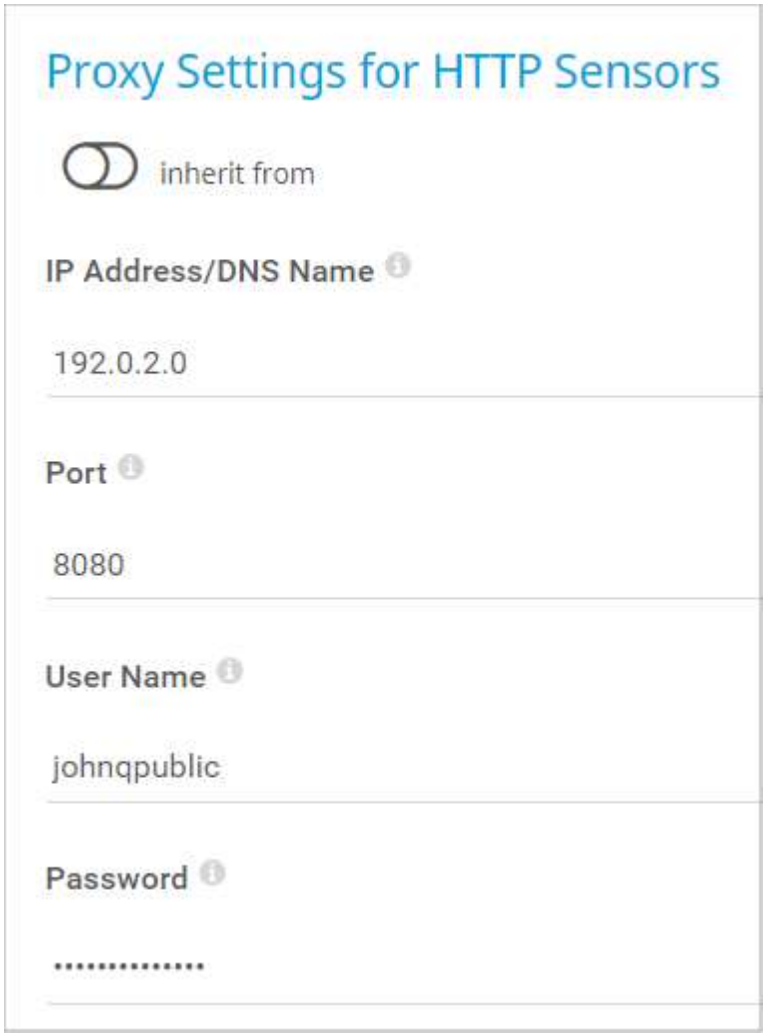
ⓘ The settings you define in this section apply to the following sensors:

- HTTP
- HTTP Advanced
- HTTP Apache ModStatus PerfStats
- HTTP Apache ModStatus Totals
- HTTP Content
- HTTP Data Advanced
- HTTP Transaction
- REST Custom

The proxy settings determine how a sensor connects to a URL. You can enter data for an HTTP proxy server that sensors use when they connect via HTTP or HTTPS.

ⓘ This setting only applies to HTTP sensors and how they monitor. To change the proxy settings for the PRTG core server, see section Core & Probes 3325.

ⓘ The SSL Certificate sensor and the SSL Security Check sensor do not support HTTP proxies but you can configure connections via SOCKS proxies in the sensors' settings:



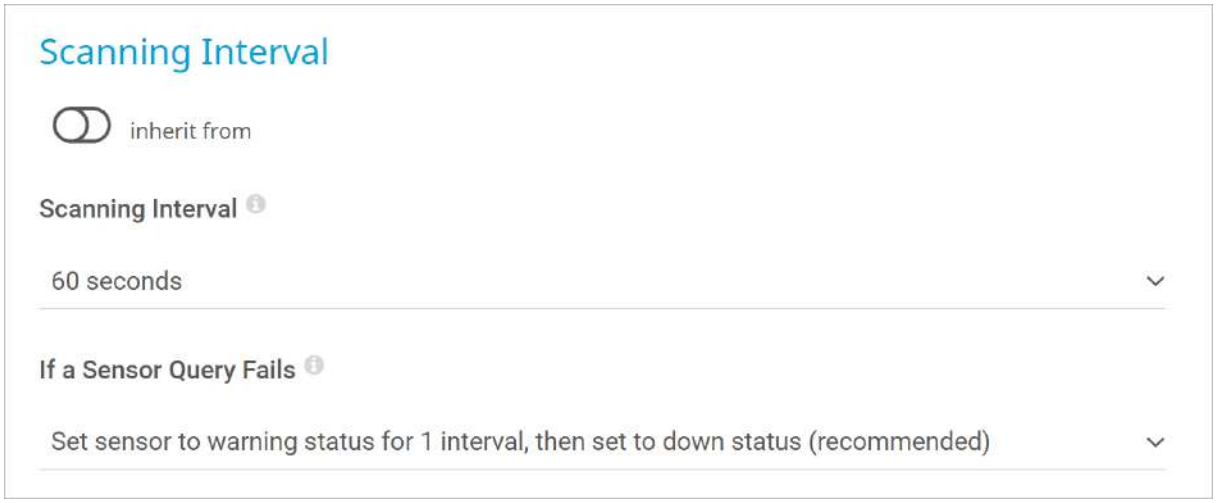
Proxy Settings for HTTP Sensors

Setting	Description
IP Address/DNS Name	Enter the IP address or Domain Name System (DNS) name of the proxy server. If you leave this field empty, HTTP sensors do not use a proxy.
Port	Enter the port number of the proxy. The default port is 8080. Enter an integer.
User Name	If the proxy requires authentication, enter the user name for the proxy login. ⓘ Only basic authentication is available. Enter a string or leave the field empty.
Password	If the proxy requires authentication, enter the password for the proxy login.

Setting	Description
	Only basic authentication is available. Enter a string or leave the field empty.

Scanning Interval

Click to interrupt the inheritance 135.



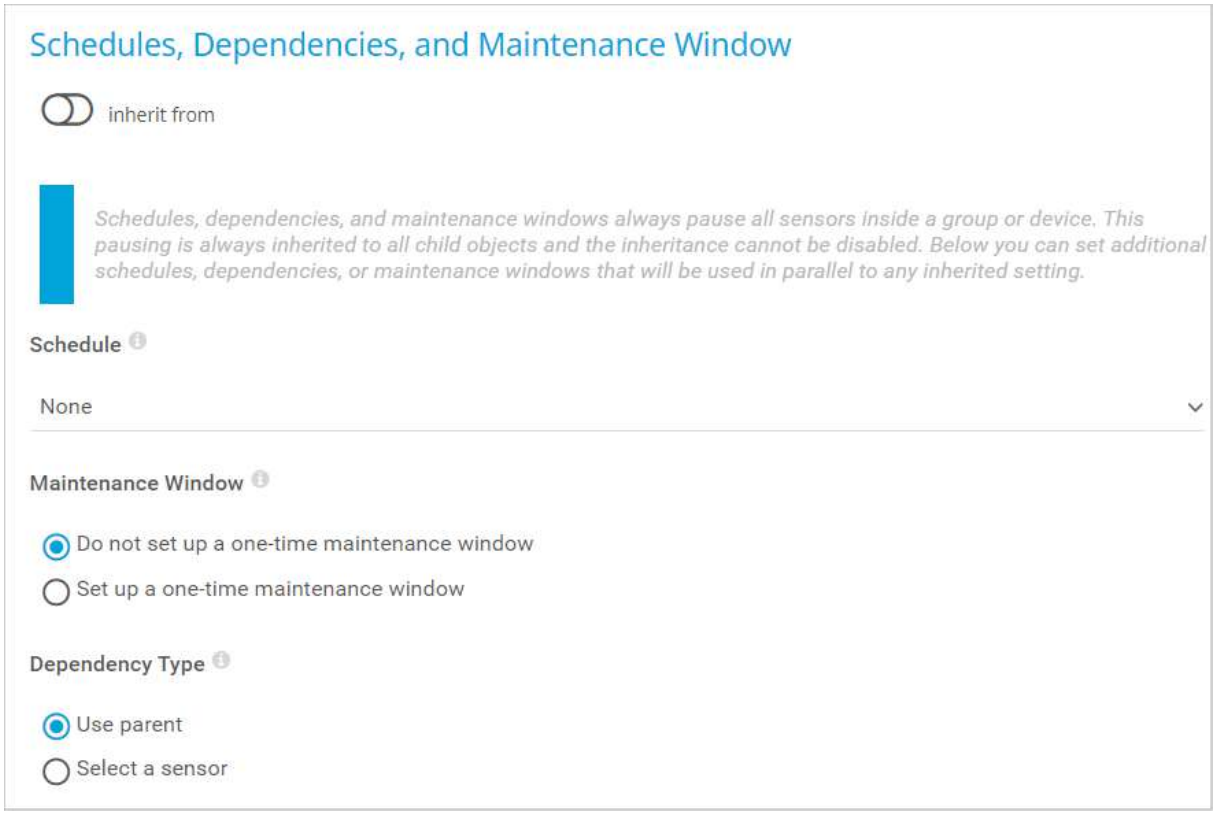
Scanning Interval

Setting	Description
Scanning Interval	Select a scanning interval from the dropdown list. The scanning interval determines the amount of time that the sensor waits between two scans. Choose from: ▪ 30 seconds ▪ 60 seconds ▪ 5 minutes ▪ 10 minutes ▪ 15 minutes ▪ 30 minutes ▪ 1 hour ▪ 4 hours ▪ 6 hours ▪ 12 hours ▪ 24 hours

Setting	Description
	ⓘ You can change the available intervals in the system administration 3307 of PRTG Network Monitor.
If a Sensor Query Fails	Select the number of scanning intervals that the sensor has time to reach and to check a device again if a sensor query fails. Depending on the option that you select, the sensor can try to reach and to check a device again several times before the sensor shows the Down status 179. This can avoid false alarms if the target device only has temporary issues. For previous scanning intervals with failed requests, the sensor shows the Warning status. Choose from: ▪ Set sensor to down status immediately: Set the sensor to the Down status immediately after the first request fails. ▪ Set sensor to warning status for 1 interval, then set to down status (recommended): Set the sensor to the Warning status after the first request fails. If the second request also fails, the sensor shows the Down status. ▪ Set sensor to warning status for 2 intervals, then set to down status: Set the sensor to the Down status only after the third request fails. ▪ Set sensor to warning status for 3 intervals, then set to down status: Set the sensor to the Down status only after the fourth request fails. ▪ Set sensor to warning status for 4 intervals, then set to down status: Set the sensor to the Down status only after the fifth request fails. ▪ Set sensor to warning status for 5 intervals, then set to down status: Set the sensor to the Down status only after the sixth request fails. ⓘ Sensors that monitor via Windows Management Instrumentation (WMI) always wait at least one scanning interval before they show the Down status. It is not possible to immediately set a WMI sensor to the Down status, so the first option does not apply to these sensors. All other options can apply. ⓘ If you define error limits for a sensor's channels, the sensor immediately shows the Down status. None of the interval options apply. ⓘ If a channel uses lookup 3604 values, the sensor immediately shows the Down status. None of the interval options apply.

Schedules, Dependencies, and Maintenance Window

Click to interrupt the inheritance 135.



Schedules, Dependencies, and Maintenance Window

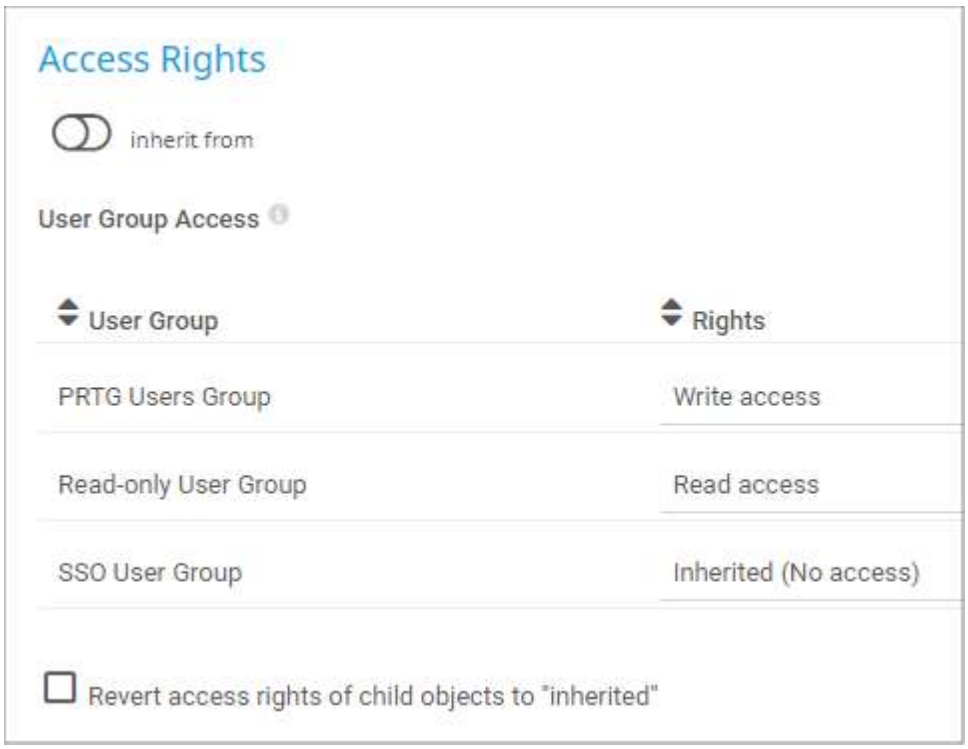
Setting	Description
Schedule	Select a schedule from the list. You can use schedules to monitor during a certain time span (days or hours) every week. Choose from: ▪ None ▪ Saturdays ▪ Sundays ▪ Weekdays ▪ Weekdays Eight-To-Eight (08:00 - 20:00) ▪ Weekdays Nights (17:00 - 09:00) ▪ Weekdays Nights (20:00 - 08:00) ▪ Weekdays Nine-To-Five (09:00 - 17:00) ▪ Weekends ⓘ You can create schedules, edit schedules, or pause monitoring for a specific time span. For more information, see section Schedules 3286.
Maintenance Window	Select if you want to set up a one-time maintenance window. During a maintenance window, monitoring stops for the selected object and all child objects. They show the Paused status instead. Choose between:

Setting	Description
	▪ Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active. ▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring. You can define a time span for the pause below. ⓘ To cancel an active maintenance window before the defined end date, change the time entry under Maintenance Ends to a date in the past.
Maintenance Begins	Select if you want to set up a one-time maintenance window. During a maintenance window, monitoring stops for the selected object and all child objects. They show the Paused status instead. Choose between: ▪ Do not set up a one-time maintenance window: Do not set up a one-time maintenance window. Monitoring is always active. ▪ Set up a one-time maintenance window: Set up a one-time maintenance window and pause monitoring. You can define a time span for the pause below.
Maintenance Ends	This setting is only visible if you enable Set up a one-time maintenance window above. Use the date time picker to enter the start date and time of the one-time maintenance window.
Dependency Type	Select a dependency type. You can use dependencies to pause monitoring for an object depending on the status of a different object. You can choose from: ▪ Use parent: Use the dependency type of the parent object. ▪ Select a sensor: Use the dependency type of the parent object. Additionally, pause the current object if a specific sensor is in the Down status or in the Paused status because of another dependency. ⓘ You do not trigger a status change by dependency if you manually pause a master object or if you pause it by schedule. ⓘ To test your dependencies 3166, select Simulate Error Status from the context menu of an object that other objects depend on. A few seconds later, all dependent objects are paused. You can check all dependencies under Devices | Dependencies in the main menu bar.
Dependency	This setting is only visible if you enable Select a sensor above. Click 🔍 and use the object selector 219 to select a sensor on which the current object will depend.
Dependency Delay (Sec.)	This setting is only visible if you select Select a sensor above. Define a time span in seconds for the dependency delay.

Setting	Description
	After the master sensor for this dependency returns to the Up status, PRTG additionally delays the monitoring of the dependent objects by the time span you define. This can prevent false alarms, for example, after a server restart or to give systems more time for all services to start. Enter an integer.

Access Rights

Click to interrupt the inheritance 135.

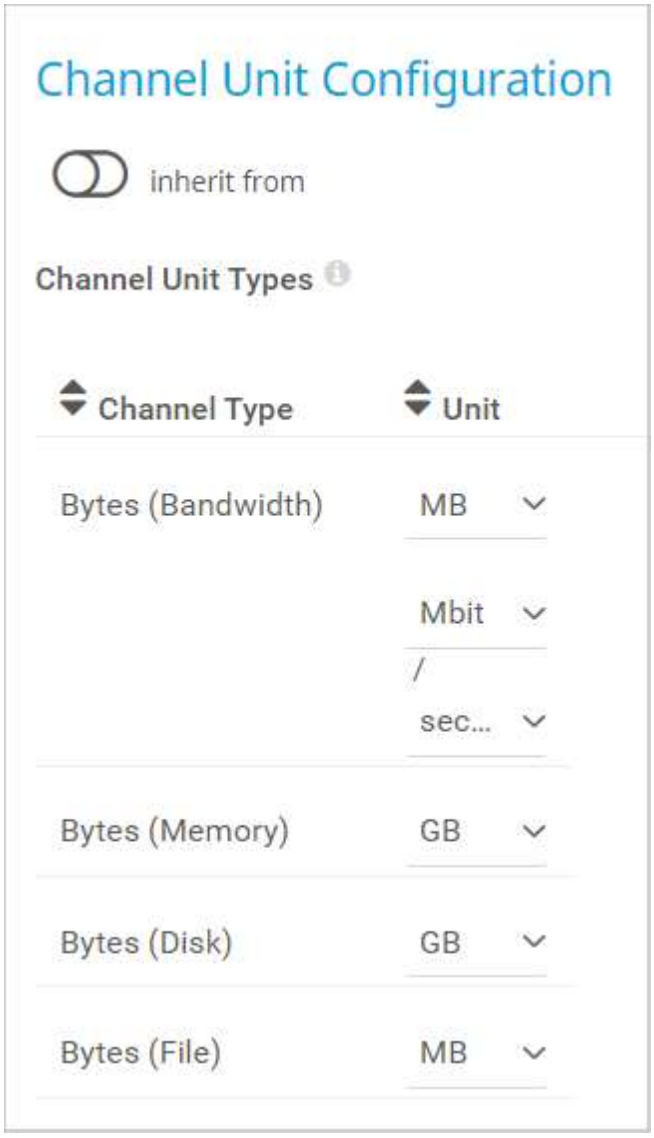


Access Rights

Setting	Description
User Group Access	Select the user groups 3346 that have access to the object. You see a table with user groups and group access rights. The table contains all user groups in your setup. For each user group, you can choose from the following group access rights: ▪ Inherited: Inherit the access rights settings of the parent object. ▪ No access: Users in this user group cannot see or edit the object. The object neither shows up in lists nor in the device tree. ⓘ There is one exception: If a user in this user group has access to a child object, the parent object is visible in the device tree but users in this user group cannot access it. ▪ Read access: Users in this group can see the object and view its monitoring results. They cannot edit any settings. ▪ Write access: Users in this group can see the object, view its monitoring results, and edit its settings. They cannot edit its access rights settings. ▪ Full access: Users in this group can see the object, view its monitoring results, edit its settings, and edit its access rights settings. To automatically set all child objects to inherit this object's access rights, enable the Revert access rights of child objects to "inherited" option. For more details on access rights, see section Access Rights Management 144.

Channel Unit Configuration

Click to interrupt the inheritance 135.

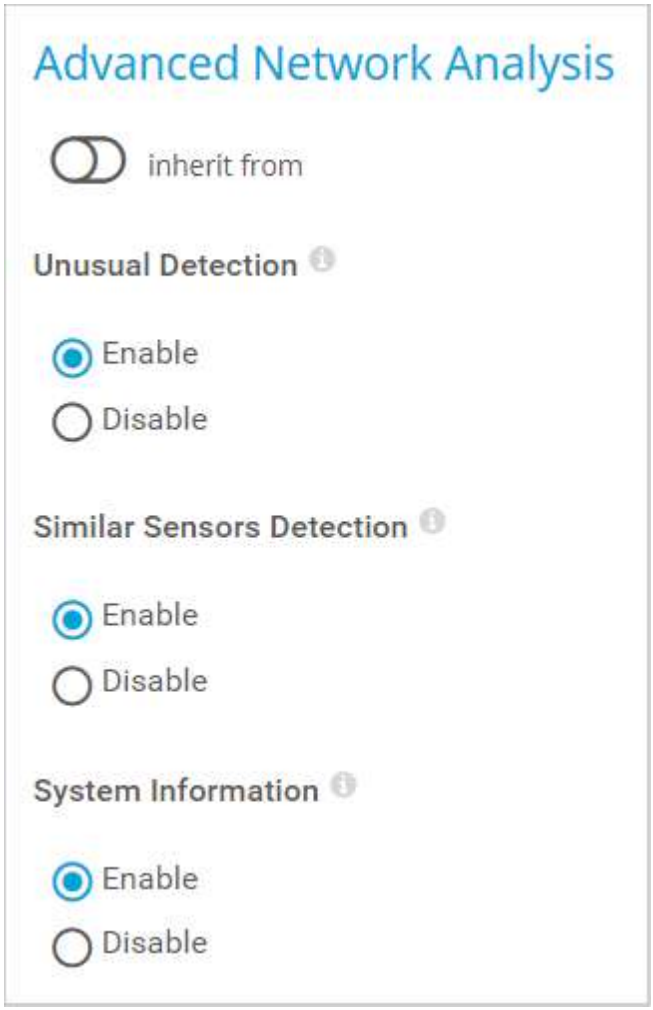


Channel Unit Configuration

For more information, see section Root Group Settings 453, section Channel Unit Configuration.

Advanced Network Analysis

Click to interrupt the inheritance 135.



Advanced Network Analysis

Setting	Description
Unusual Detection	Select if you want to use the unusual detection 3309 for sensors: ▪ Enabled: Activates the unusual detection for this object and, by default, for all objects underneath in the object hierarchy 131. Sensors that are affected by this setting show the Unusual status if PRTG detects unusual activity. ▪ Disabled: Does not activate the unusual detection. PRTG ignores unusual values for sensors that are affected by this setting. These sensors do not show the Unusual status. ⓘ You can configure the behavior of the unusual detection or completely disable it in the system settings 3309.
Similar Sensors Detection	Select if you want to activate the similar sensors 189 analysis:

Setting	Description
	▪ Enabled: Activates the similar sensors detection for this object and, by default, for all objects underneath in the object hierarchy. PRTG considers all sensors that are affected by this setting during the similarity analysis. ▪ Disabled: Does not activate the similar sensors detection. PRTG does not consider sensors that are affected by this setting during the similarity analysis. ⓘ You can configure the depth of the analysis of the similar sensors detection or completely disable it in the system settings 3311.
System Information	Select if you want to retrieve and show system information 202 for your devices: ▪ Enabled: Activates the system information feature for this object and, by default, for all objects underneath in the hierarchy. ▪ Disabled: Does not activate the system information feature. ⓘ The System Information feature is enabled by default. To retrieve the data, PRTG automatically uses the credentials for Windows systems 596 and the credentials for SNMP devices 603 that you entered in the device settings or that the device inherits 131 from a parent object like the root group. Consider this when you monitor devices that are outside of your local network, especially when you use SNMP v1 or SNMP v2c, which do not provide encryption. ☁ This setting is not available on the hosted probe of a PRTG Hosted Monitor instance.

ⓘ Save your settings. If you change tabs or use the main menu without saving, all changes to the settings are lost.

More

KNOWLEDGE BASE

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- https://kb.paessler.com/en/topic/38083

Where can I find the Web Services API (WSAPI) port for the connection to the HPE 3PAR system?

- https://kb.paessler.com/en/topic/89717

How do I obtain credentials and set permissions for the Microsoft 365 Service Status sensors?

- https://kb.paessler.com/en/topic/88462

How do I obtain credentials and create custom roles for the Microsoft Azure sensors?

- https://kb.paessler.com/en/topic/88625

What is the Overflow Values setting in the SNMP Compatibility Options?

- https://kb.paessler.com/en/topic/43503

How can I change the defaults for names automatically generated for new SNMP sensors?

- https://kb.paessler.com/en/topic/7363

Automatically update port name and number for SNMP Traffic sensors when the device changes them

- https://kb.paessler.com/en/topic/25893

7.8 Sensor Settings

There is a dedicated section for every sensor with details about the available settings.

- For more information, see section List of Available Sensor Types.

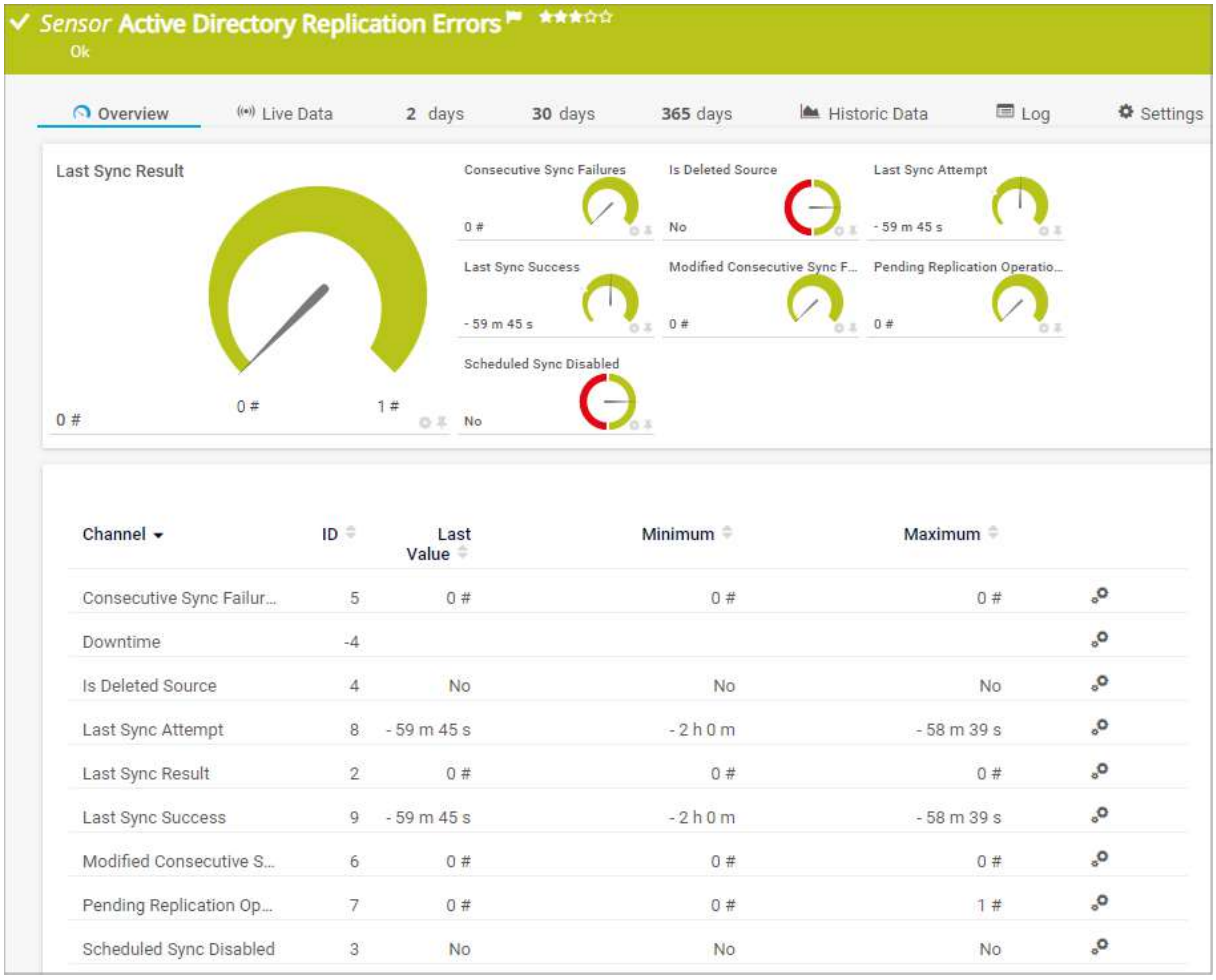
- For sensor settings, multi-edit is also available. This enables you to change properties of many sensors at the same time. For more information, see section Multi-Edit.

To detect unexpected correlations between your network components, PRTG provides a similar sensors analysis.

ⓘ Usually, a sensor connects to the IP Address/DNS Name of the parent device. See the device settings for details. For some sensors, you can explicitly define the monitoring target in the sensor settings.

7.8.1 Active Directory Replication Errors Sensor

The Active Directory Replication Errors sensor checks a Windows domain controller (DC) for replication errors.



Active Directory Replication Errors Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section Channel List 660.

Sensor in Other Languages

- Dutch: Active Directory Replicatie Fouten
- French: Active Directory erreurs de réplication
- German: Active Directory Replikationsfehler
- Japanese: AD レプリケーションエラー監視
- Portuguese: Erros de replicação Active Directory
- Russian: Ошибки репликации Active Directory
- Simplified Chinese: 活动目录复制错误
- Spanish: Errores de replicación Active Directory

Remarks

- This sensor has a high performance impact. We recommend that you use no more than 200 of this sensor on each probe.
- This sensor requires 655 the probe system to be part of the domain whose Active Directory you want to monitor.
- This sensor requires 655 .NET 4.7.2 or later from Microsoft on the probe system. If the sensor shows the error PE087, additionally install .NET 3.5 on the probe system.
- We recommend Windows Server 2012 R2 on the probe system for best performance of this sensor.
- This sensor requires that the parent device is a DC.
- This sensor requires credentials for Windows systems in the settings of the parent device.
- This sensor supports IPv6.
- This sensor uses lookups to determine the status values of one or more channels.

You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

Detailed Requirements

Requirement	Description
Member of Windows domain	This sensor only works if the probe system is part of the domain whose Active Directory you want to monitor. You must add the sensor to a device that represents the DC.
.NET 4.7.2 or later	This sensor requires .NET 4.7.2 or later to be installed on the probe system (on every cluster node, if on a cluster probe). If the framework is missing, you cannot create this sensor. For more information, see the Knowledge Base: Which .NET version does PRTG require?
Windows credentials	This sensor requires credentials for Windows systems in the settings of the parent device. We recommend that you use Windows domain credentials. If you use local credentials, make sure that the same Windows user accounts (with the same user name and password) exist on both the probe system and the target system. Otherwise, the sensor cannot correctly connect.

Basic Sensor Settings

Basic Sensor Settings

Setting	Description
Sensor Name	Enter a name to identify the sensor. By default, PRTG shows this name in the device tree, as well as in alarms, logs, notifications, reports, maps, libraries, and tickets. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Parent Tags	The tags that the sensor inherits from its parent device, parent group, and parent probe. ⓘ This setting is for your information only. You cannot change it.
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically inherited. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added. The sensor has the following default tags that are automatically predefined in the sensor's settings when you add the sensor: ▪ ptfsensor
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

Sensor Settings

Sensor Settings

Setting	Description
Replication Neighbor	The replication neighbor whose replication connection this sensor monitors.
Naming Context	Select the Active Directory naming context that you want to monitor: ▪ Configuration (default): Includes information about partitions, sites, services, or the Active Directory schema. ▪ Schema: Includes the information by which objects, classes, and attributes that are used in the Active Directory are defined. ▪ DomainDnsZones: Includes information about the domain controllers that are in the domain. ▪ Domain: Includes domain information that is replicated to this domain's domain controllers, for example information about computers or users. ⓘ The probe system must be part of the domain whose naming context you want to monitor. ▪ ForestDnsZones: Includes information about domain controllers in the forest. ⓘ You cannot change this value after sensor creation.

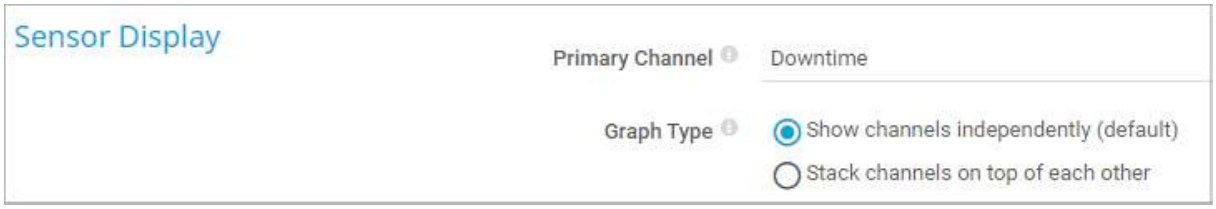
Debug Options

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: ▪ Discard result: Do not store the sensor result.

Setting	Description
	▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the PRTG data directory on the probe system. The file names are Result of Sensor [ID].txt and Result of Sensor [ID].Data.txt. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval. ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.

Sensor Display



Sensor Display

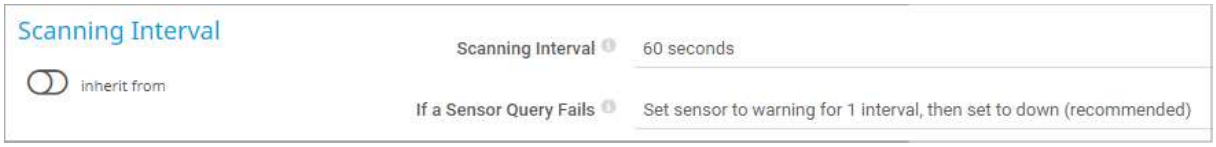
Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel is always displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set a different primary channel later by clicking 📌 below a channel gauge on the sensor's Overview tab.
Graph Type	Define how different channels are shown for this sensor: ▪ Show channels independently (default): Show a graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings).
Stack Unit	This setting is only visible if you enable Stack channels on top of each other as Graph Type. Select a unit from the list. All channels with this unit are stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section Inheritance of Settings.

Scanning Interval

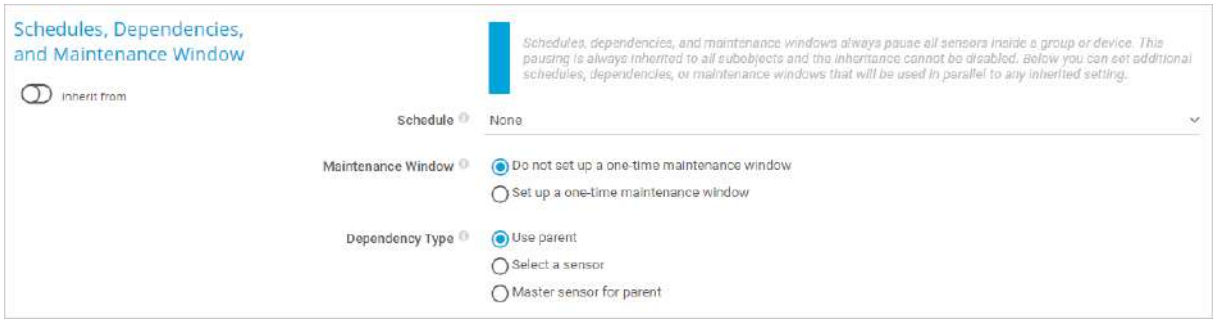


Scanning Interval

For more information, see section Root Group Settings, section Scanning Interval.

Schedules, Dependencies, and Maintenance Window

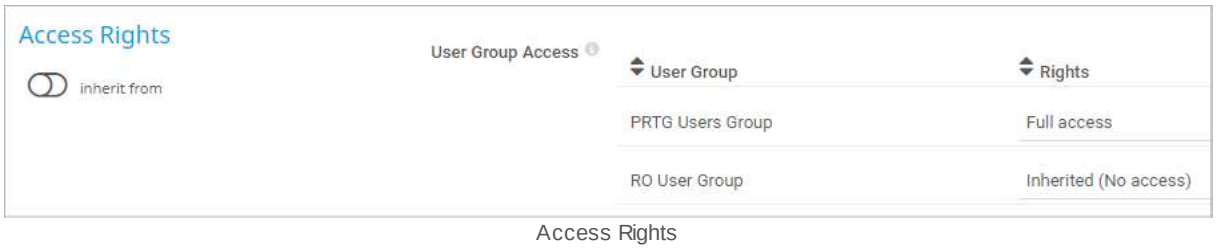
You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.



Schedules, Dependencies, and Maintenance Window

For more information, see section Root Group Settings, section Schedules, Dependencies, and Maintenance Window.

Access Rights

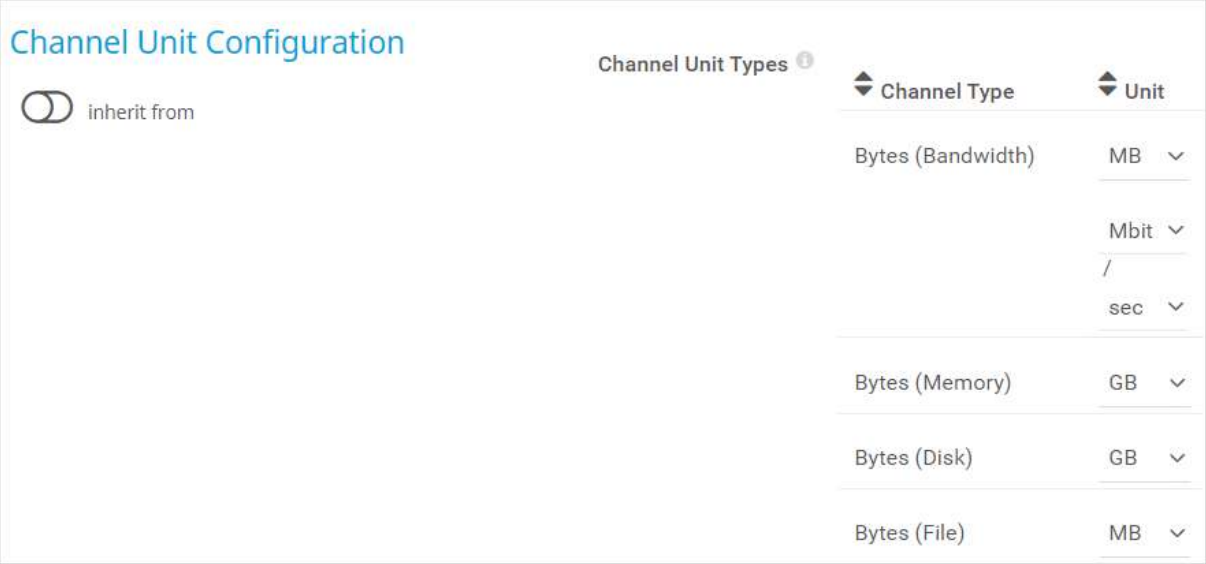


Access Rights

For more information, see section Root Group Settings, section Access Rights.

Channel Unit Configuration

Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.



Channel Unit Configuration

For more information, see section Root Group Settings, section Channel Unit Configuration.

Channel List

Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Setting	Description
Consecutive Sync Failures	The number of consecutive synchronization failures
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Is Deleted Source	If the source is deleted ▪ Up status: No ▪ Down status: Yes
Last Sync Attempt	The time of the last synchronization attempt

Setting	Description
Last Sync Result	The result of the last synchronization ⓘ This channel is the primary channel by default.
Last Sync Success	The time of the last synchronization success
Modified Consecutive Sync Failures	The number of modified, consecutive synchronization failures
Pending Replication Operations	The number of pending replication operations
Scheduled Sync Disabled	If the scheduled synchronization is disabled ▪ Up status: No ▪ Down status: Yes

More

KNOWLEDGE BASE

Which .NET version does PRTG require?

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

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

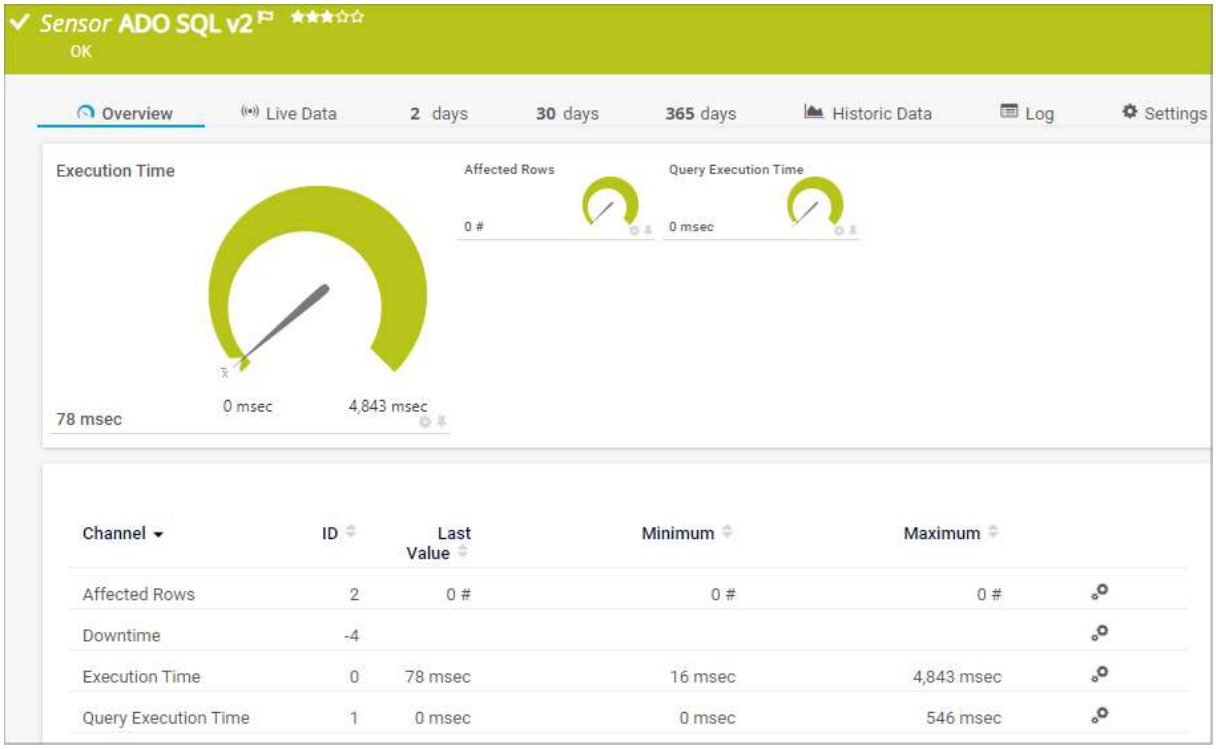
How do I monitor Active Directory (AD) replication without domain admin rights?

- https://kb.paessler.com/en/topic/91620

7.8.2 ADO SQL v2 Sensor

The ADO SQL v2 sensor monitors a database via an ActiveX Data Objects (ADO) connection and it executes a Structured Query Language (SQL) query.

ⓘ The sensor can monitor any data source that is available via Object Linking and Embedding, Database or Open Database Connectivity (ODBC).



ADO SQL v2 Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section Channel List 673.

Sensor in Other Languages

- Dutch: ADO SQL v2
- French: ADO SQL v2
- German: ADO SQL v2
- Japanese: ADO SQL v2
- Portuguese: ADO SQL v2
- Russian: ADO SQL v2
- Simplified Chinese: ADO SQL v2
- Spanish: ADO SQL v2

Remarks

- This sensor has a high performance impact. We recommend that you use no more than 200 of this sensor on each probe.

- This sensor requires that the Structured Query Language (SQL) query is stored in a file on the probe system. In a cluster, copy the file to every cluster node.
- This sensor requires 663 .NET 4.7.2 or later from Microsoft on the probe system.
- If you use an ODBC connection, define the ODBC connection in the Windows ODBC Connection Manager first. If it is a 64-bit Windows, define the ODBC connection as an ODBC 32-bit connection.
- This sensor supports IPv6.
- This sensor can use lookups 668. Select Lookup as Channel #x Unit and define the lookup file in Channel #x Lookup.
- Define the credentials for database management systems in settings that are higher in the object hierarchy.
- Knowledge Base: How to set up the SQL v2 sensors in PRTG? Is there a guide?
- Knowledge Base: How can I monitor strings from an SQL database and show a sensor status depending on it?
- Knowledge Base: How can I monitor error tables in SQL databases?
- Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

You cannot add this sensor to the hosted probe of a PRTG Hosted Monitor instance. If you want to use this sensor, add it to a remote probe device.

Detailed Requirements

Requirement	Description
.NET 4.7.2 or later	This sensor requires .NET 4.7.2 or later to be installed on the probe system (on every cluster node, if on a cluster probe). If the framework is missing, you cannot create this sensor. For more information, see the Knowledge Base: Which .NET version does PRTG require?

Basic Sensor Settings

Basic Sensor Settings

Setting	Description
Sensor Name	Enter a name to identify the sensor. By default, PRTG shows this name in the device tree, as well as in alarms, logs, notifications, reports, maps, libraries, and tickets. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Parent Tags	The tags that the sensor inherits from its parent device, parent group, and parent probe. ⓘ This setting is for your information only. You cannot change it.
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically inherited. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added. The sensor has the following default tags that are automatically predefined in the sensor's settings when you add the sensor: ▪ sqlsensor
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

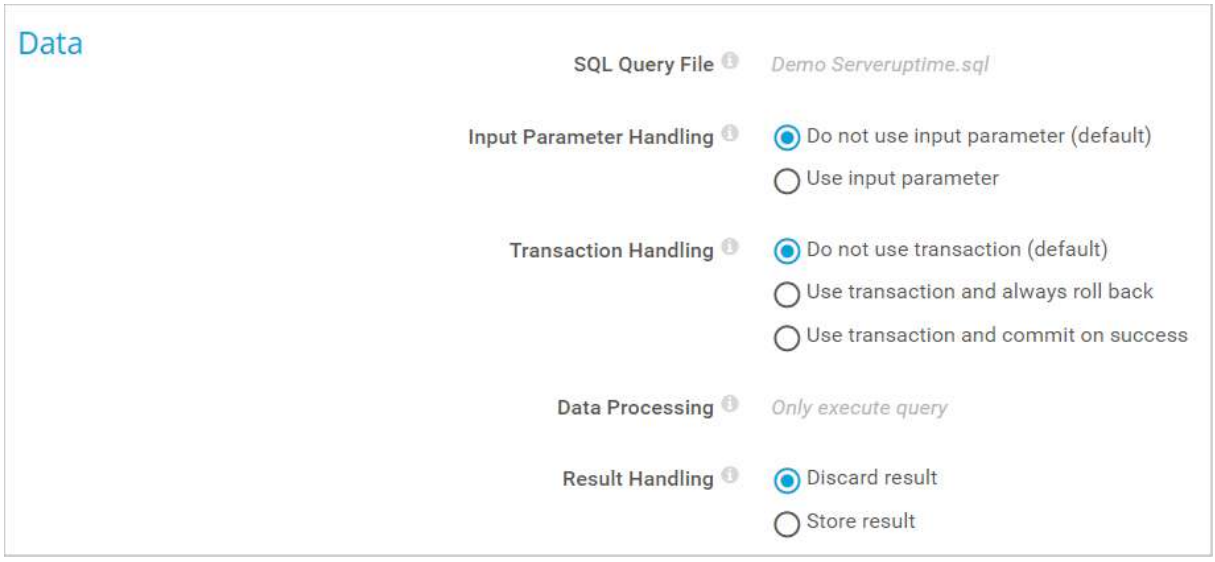
Database Specific

Database Specific

Setting	Description
Connection String	Enter the connection string that the sensor uses to connect to the database. A connection string can look like this, for example:

Setting	Description
	Provider=SQLOLEDB.1;Data Source=10.0.0.200\SQLEXPRESS;User ID=user;Password=userpass;Initial Catalog=Northwind For ODBC connections, you must enter MSDASQL as provider, for example Provider=MSDASQL;DSN=_my_odbc_sqlserver. You can use the placeholders %dbloginuser and %dbloginpassword. PRTG replaces them with the credentials for database management systems of the parent device.

Data



Sensor Display

Setting	Description
SQL Query File	Select the SQL query file that includes a valid SQL statement that the sensor executes on the server with every scanning interval. The list contains SQL scripts from the \Custom Sensors\sql subfolder of the PRTG program directory on the probe system. Store your script there. If you use the script on a cluster probe, you must store the script on all cluster nodes. A correct expression in the file could be: SELECT AVG(UnitPrice) FROM Products. If you want to use transactions, separate the individual steps with semicolons ";". Note that with each request, PRTG transfers the full result set, so use filters and limits in your query. The demo script Demo Serveruptime.sql is available by default. You can use it to monitor the uptime of the target server.

Setting	Description
	See also the Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer? You cannot change this value after sensor creation.
Input Parameter Handling	Define if you want to pass a parameter to the SQL query file: ▪ Do not use input parameter (default): Execute the SQL query file without using variables. ▪ Use input parameter: Execute an SQL query file that contains a variable. Provide the parameter that you want to use in the query below.
Input Parameter	This setting is only visible if you select Input Parameter Handling above. Enter the parameter that you want to pass to the SQL query file. This parameter replaces the variables @prtg, :prtg, or ? in the SQL query, considering the general rules for SQL variables. You can also use PRTG placeholders for custom sensors (command-line parameters) as input parameters, for example, %sensorid or %deviceid. For details, see section Custom Sensors. Provide strings as they are and do not surround them with quotation marks. PRTG automatically and correctly inserts string parameters into the query.
Transaction Handling	Define if you want to use transactions and if they affect the database content: ▪ Do not use transaction (default): Do not execute transactions. ▪ Use transaction and always roll back: The query does not change data in the database. In the SQL query file, separate the single steps of the transaction with semicolons. ▪ Use transaction and commit on success: The query changes data in the database. The changes only apply if all execution steps succeed without any errors. In the SQL query file, separate the single steps of the transaction with semicolons.
Data Processing	Define whether the sensor processes data from the database: ▪ Only execute query: Only show information about the number of affected rows and the execution time of the query. Affected rows are rows that were changed by the query (for example, created, deleted, or edited). ▪ Count table rows: Execute a SELECT statement and monitor how many rows of the data table this statement returns. ▪ Process data table: Read and analyze the data table. If you select this option, the sensor counts rows with SELECT statements as well.

Setting	Description
	ⓘ You cannot change this value after sensor creation.
DBNull Handling	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation. Define the sensor behavior if the query returns DBNull: ▪ Error: Show a Down status if the query returns DBNull. ▪ Number 0: Recognize the result DBNull as a valid value and interpret it as the number 0.
Select Channel Value by	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation. Define how to select the desired cell in the database table: ▪ Column number: Determine the channel value by using the value in row 0 of the column whose number you specify in Channel #x Column Number. ▪ Column name: Determine the channel value by using the value in row 0 of the column whose name you specify in Channel #x Column Name. ▪ Row number: Determine the channel value by using the value in column 0 of the row whose number you specify in Channel #x Row Number. ▪ Key value pair: Determine the channel value by searching in column 0 for the key you specify in Channel #x Key and by returning the value in column 1 of the same row where the key value was found. ⓘ Defining how the desired cell in the database table is selected is necessary to configure the cells that are used in the channels. ⓘ The option you select here also defines the method of how to optionally determine a value for the sensor message. For details, see setting Use Data Table Value in Message. For an example for channel value selection, see section Monitoring Databases.
Channel #2 - #10	This setting is only visible if you select Process data table above. You can define up to 10 channels. You must define at least one data channel, so you see all available settings for Channel #1. Specify how to handle all other possible channels: ▪ Disable: Do not create this channel. ▪ Enable: Create this channel. ⓘ It is not possible to enable or disable channels after sensor creation.

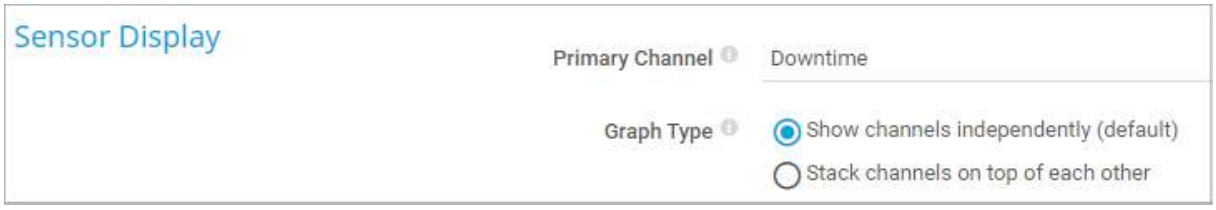
Setting	Description
Channel #x Name	This setting is only visible if you select Process data table above. Enter a name for the channel. Enter a string. The sensor dynamically generates channels with this name as identifier. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Channel #x Column Number	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column number for the setting Select Channel Value by. Provide the number of the column to use to determine the channel value in row 0. Enter an integer.
Channel #x Column Name	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Column name for the setting Select Channel Value by. Provide the name of the column to use to determine the channel value in row 0. Enter an integer.
Channel #x Row Number	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Row number for the setting Select Channel Value by. Provide the number of the column to use to determine the channel value in row 0. Enter an integer.
Channel #x Key	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation and if you select Key value pair for the setting Select Channel Value by. Provide the key to search for in column 0 of the data table. The value in column 1 of the same row where the key value was found to use to determine the channel value. Enter a string.
Channel #x Mode	This setting is only visible if you select Process data table above. Define how to display the determined value in the channel: ▪ Absolute (recommended): Show the value as the sensor retrieves it from the data table. ▪ Difference: The sensor calculates and shows the difference between the last and the current value returned from the data table. ⓘ This mode is not compatible with the unit Lookup. ⓘ This mode only works if the difference between the last and the current value is positive and increases with each scanning interval. This mode does not support negative and decreasing values. ⓘ You cannot change this value after sensor creation.
Channel #x Unit	This setting is only visible if you select Process data table above. Define the unit of the channel value: ▪ BytesBandwidth

Setting	Description
	▪ BytesMemory ▪ BytesDisk ▪ Temperature ▪ Percent ▪ TimeResponse ▪ TimeSeconds ▪ TimeHours ▪ Count ▪ CPU ▪ BytesFile ▪ SpeedDisk ▪ SpeedNet ▪ Custom ▪ Lookup For more information about the available units, see section Custom Sensors. To use lookups with this channel, select Lookup and define the lookup file in Channel #x Lookup. Do not use Custom if you use lookups with this sensor. It is not possible to use the unit Lookup in combination with the Difference mode. You are not able to create the sensor in this case.
Channel #x Custom Unit	This setting is only visible if you select the channel unit Custom above. Define a unit for the channel value. Enter a string.
Channel #x Lookup	This setting is only visible if you select the channel unit Lookup above. Select a lookup file that you want to use with this channel.
Use Data Table Value in Message	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation. Define if the sensor message shows a value from the data table: ▪ Disable: Do not use a custom sensor message. ▪ Enable: Define a custom sensor message with a defined value of the data table. Define the value selection below. The method of how to determine a value for the sensor message is defined in the setting Select Channel Value by above.

Setting	Description
Message Column Number	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column number for the setting Select Channel Value by, and if you enable Use Data Table Value in Message. Enter the number of a column. The sensor message shows the value in row 0 of this column. Enter an integer.
Message Column Name	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Column name for the setting Select Channel Value by, and if you enable Use Data Table Value in Message. Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter a string. ⓘ Columns start with index 0.
Message Row Number	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Row number for the setting Select Channel Value by, and if you enable Use Data Table Value in Message. Enter the name of a column. The sensor message shows the value in row 0 of this column. Enter the number of a row. The sensor message shows the value in column 0 of this row. Enter an integer. ⓘ Rows start with index 0.
Message Key	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation, if you select Key value pair for the setting Select Channel Value by, and if you enable Use Data Table Value in Message. Enter a key to search for in column 0 of the data table. The sensor message shows the value in column 1 of the row where the key was found. Enter a string.
Message	This setting is only visible if you enable Use Data Table Value in Message. Define the sensor message. Enter a string. Use the placeholder {0} at the position where you want to display the value. Example: The message is {0} ⓘ The number sign (#) is not supported in sensor messages. If a message contains a number sign, the message is clipped at this point.
If Message Changes	This setting is only visible if you select Process data table for the setting Data Processing during sensor creation. Define what the sensor does when its message changes: ▪ Ignore (default): Do nothing.

Setting	Description
	▪ Trigger 'change' notification: Send an internal message that indicates a change. ⓘ In combination with a change trigger, you can use this to trigger a notification if a change occurs.
Result Handling	Define what PRTG does with the sensor result: ▪ Discard result: Do not store the sensor result. ▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the PRTG data directory on the probe system. The file names are Result of Sensor [ID].txt, Result of Sensor [ID].Data.txt, and Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites these files with each scanning interval. ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.

Sensor Display



Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel is always displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set a different primary channel later by clicking 📌 below a channel gauge on the sensor's Overview tab.
Graph Type	Define how different channels are shown for this sensor: ▪ Show channels independently (default): Show a graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings).

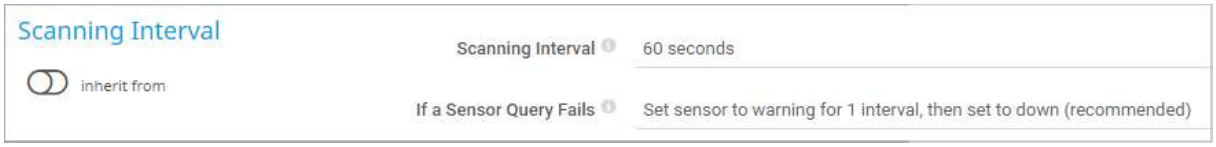
Setting	Description
Stack Unit	This setting is only visible if you enable Stack channels on top of each other as Graph Type. Select a unit from the list. All channels with this unit are stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

For more information, see section Inheritance of Settings.

Scanning Interval

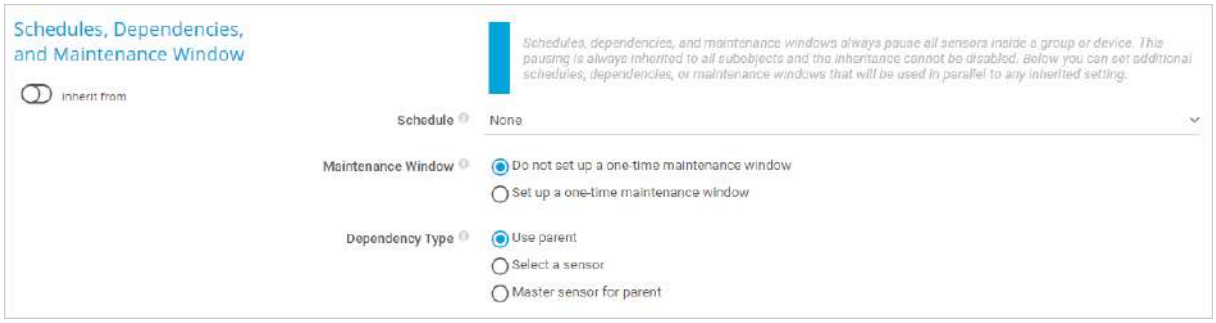


Scanning Interval

For more information, see section Root Group Settings, section Scanning Interval.

Schedules, Dependencies, and Maintenance Window

You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.

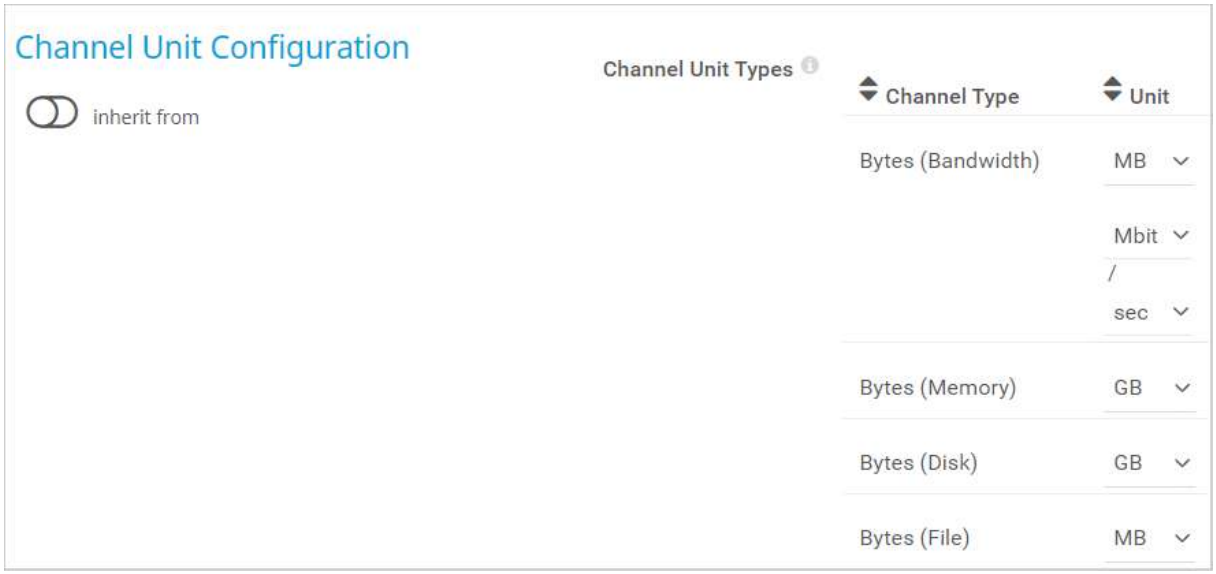


Schedules, Dependencies, and Maintenance Window

For more information, see section Root Group Settings, section Schedules, Dependencies, and Maintenance Window.

Channel Unit Configuration

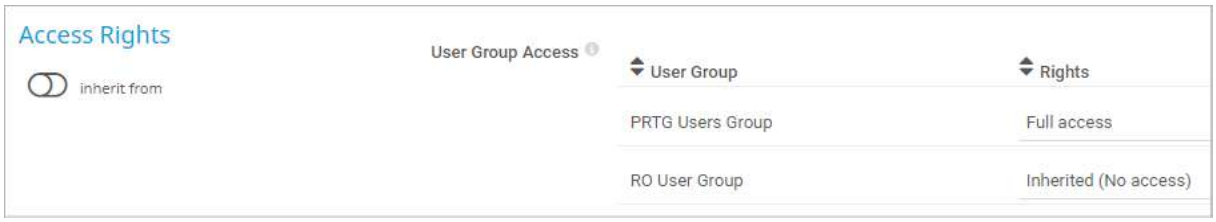
ⓘ Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.



Channel Unit Configuration

For more information, see section Root Group Settings, section Channel Unit Configuration.

Access Rights



Access Rights

For more information, see section Root Group Settings, section Access Rights.

Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Affected Rows	The number of rows that were addressed by the query (including SELECT statements if you process data tables)

Channel	Description
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Execution Time	The execution time of the entire request (including connection buildup, query execution, transaction handling, disconnection) ⓘ This channel is the primary channel by default.
Query Execution Time	The execution time of the specified query

SQL Variables

You can use the following variables in the SQL query file to be replaced by an input parameter. This is useful if you have various SQL sensors with queries that differ in only one parameter.

- Microsoft SQL, MySQL, PostgreSQL: @prtg
- Oracle SQL: :prtg
- ADO SQL: ? (question mark)

ⓘ @prtg, :prtg, and ? are common SQL query parameters and they are used in a parameterized SQL query. This means that the query and the parameter are forwarded without any changes to the database. This leads to some restrictions on the database side. For example, you cannot use variables as placeholders for table names or as lists in IN operators.

Examples for variables usage:

```
SELECT * FROM Table WHERE name = @prtg
```

```
SELECT @prtg FROM Table
```

More

KNOWLEDGE BASE

How to set up the SQL v2 sensors in PRTG? Is there a guide?

- https://kb.paessler.com/en/topic/70618

How can I monitor strings from an SQL database and show a sensor status depending on it?

- https://kb.paessler.com/en/topic/63259

How can I monitor error tables in SQL databases?

- https://kb.paessler.com/en/topic/70774

Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?

- https://kb.paessler.com/en/topic/75372

Which .NET version does PRTG require?

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

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

How do I monitor the size of a Microsoft SQL Server database?

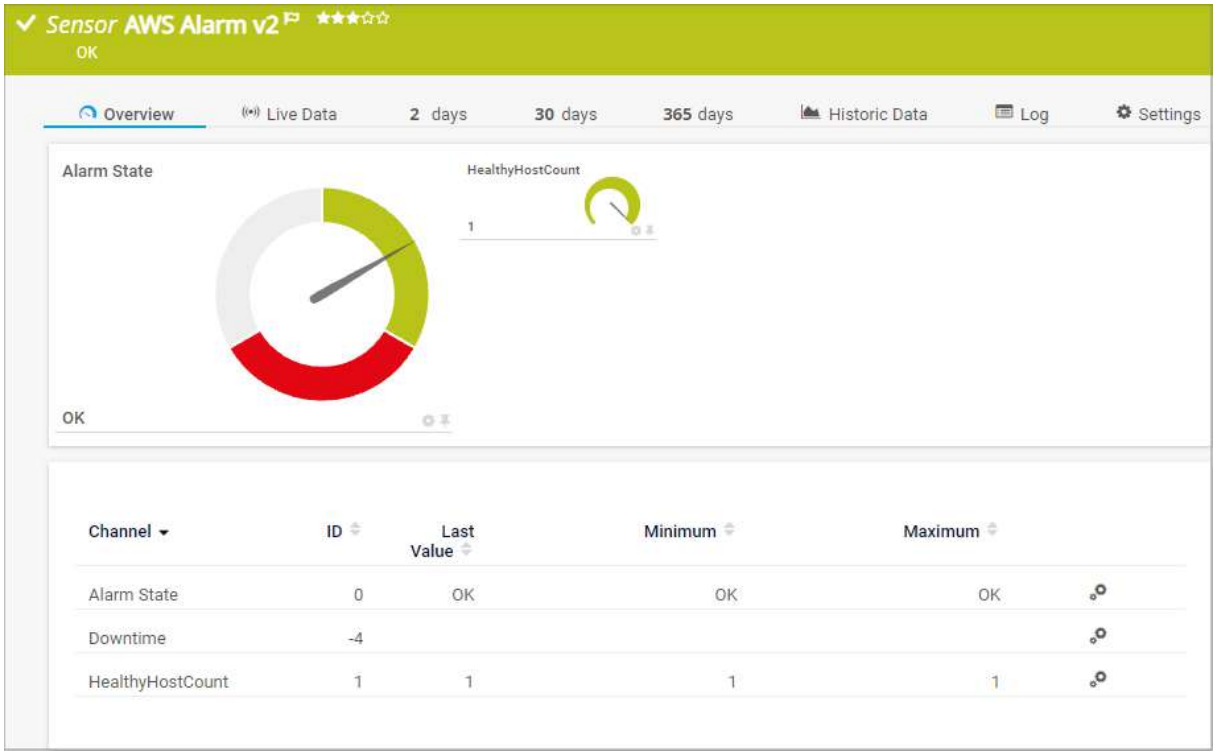
- https://kb.paessler.com/en/topic/18183

7.8.3 AWS Alarm v2 Sensor

The AWS Alarm v2 sensor monitors the status of an Amazon Web Services (AWS) alarm by reading its data from Amazon CloudWatch via the AWS API.

If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

If you monitor an AWS alarm that is based on a metric math expression, the sensor does not create an additional channel that monitors the math expression.



AWS Alarm v2 Sensor

For a list of regions that this sensor supports, see section List of Supported AWS Regions and Their Codes.

For a detailed list and descriptions of the channels that this sensor can show, see section Channel List 682.

Sensor in Other Languages

- Dutch: AWS Alarm v2
- French: AWS Alarm v2
- German: AWS Alarm v2
- Japanese: AWS Alarm v2
- Portuguese: AWS Alarm v2
- Russian: AWS Alarm v2

- Simplified Chinese: AWS Alarm v2
- Spanish: Alarma AWS v2

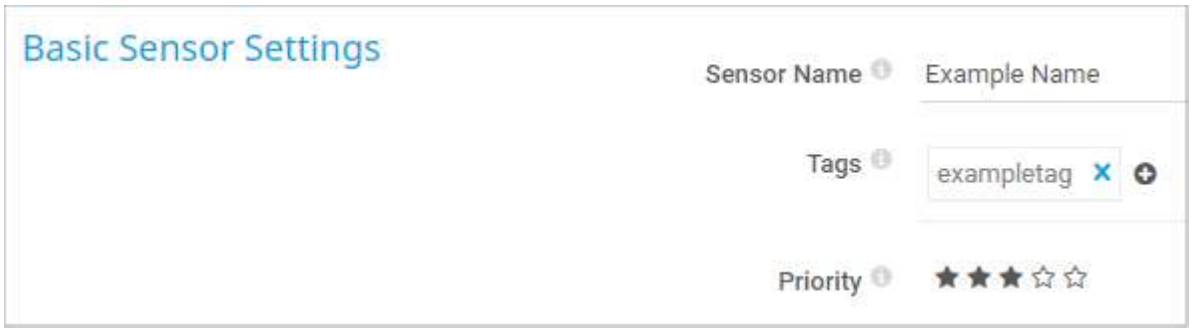
Remarks

- This sensor requires 677 permissions for the AWS API key.
- This sensor requires credentials for AWS in settings that are higher in the object hierarchy.
- This sensor supports MetricAlarm and CompositeAlarm.
- This sensor supports IPv6.
- This sensor has a low performance impact.
- This sensor uses lookups to determine the status values of one or more channels.
- Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see Amazon CloudWatch Pricing – Amazon Web Services (AWS).
- It can take up to several minutes before objects appear in the Add Sensor dialog.

Detailed Requirements

Requirement	Description
Permissions for the AWS API key	This sensor requires sufficient rights to query data from the AWS API For more information, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

Basic Sensor Settings



Basic Sensor Settings

Setting	Description
Sensor Name	Enter a name to identify the sensor.

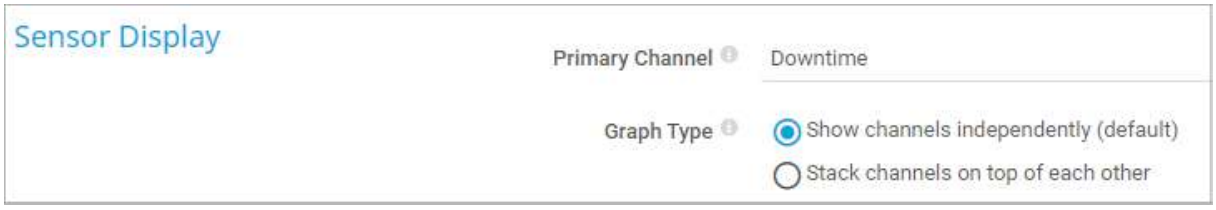
Setting	Description
Parent Tags	The tags that the sensor inherits from its parent device, parent group, and parent probe. ⓘ This setting is for your information only. You cannot change it.
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically inherited. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added. The sensor has the following default tags that are automatically predefined in the sensor's settings when you add the sensor: ▪ aws ▪ cloudwatch ▪ alarm ▪ cloudwatchsensor
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

AWS Alarm Specific

AWS Alarm Specific

Setting	Description
Name	The name of the AWS alarm that this sensor monitors.
Type	The type of the AWS alarm that this sensor monitors.
Description	The description of the AWS alarm that this sensor monitors.
Region	The region in which the AWS alarm that this sensor monitors occurs. For a list of regions that this sensor supports, see section List of Supported AWS Regions and Their Codes.

Sensor Display



Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel is always displayed below the sensor's name. The available options depend on what channels are available for this sensor. You can set a different primary channel later by clicking below a channel gauge on the sensor's Overview tab.
Graph Type	Define how different channels are shown for this sensor: ▪ Show channels independently (default): Show a graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings).
Stack Unit	This setting is only visible if you enable Stack channels on top of each other as Graph Type. Select a unit from the list. All channels with this unit are stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Debug Options

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: ▪ Discard result: Do not store the sensor result. ▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the PRTG data directory on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval. This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance. In a cluster, PRTG stores the result in the PRTG data directory of the master node.

Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

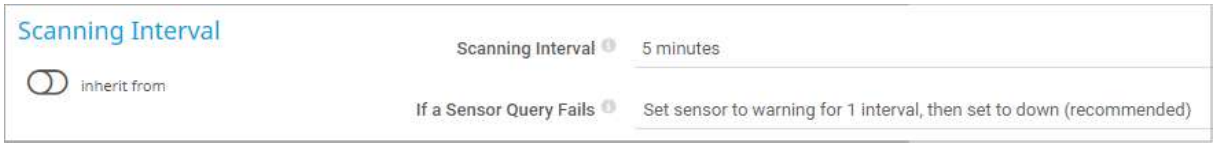
For more information, see section Inheritance of Settings.

Scanning Interval

This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the Monitoring settings are not available for this sensor.

The minimum scanning interval of this sensor is 1 minute.

The recommended scanning interval of this sensor is 5 minutes.

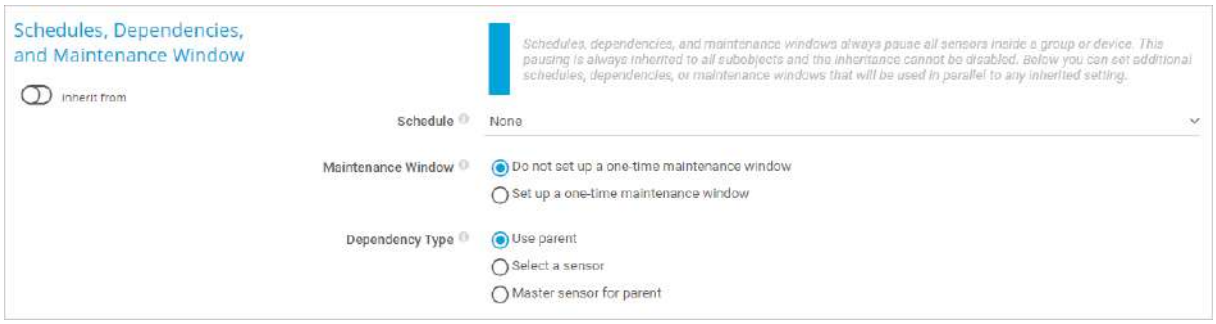


Scanning Interval

For more information, see section Root Group Settings, section Scanning Interval.

Schedules, Dependencies, and Maintenance Window

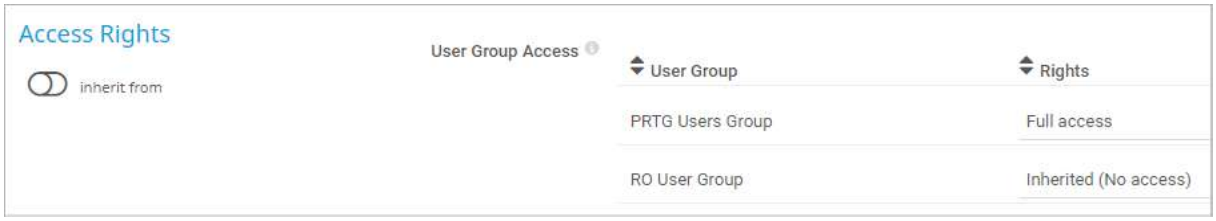
You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.



Schedules, Dependencies, and Maintenance Window

For more information, see section Root Group Settings, section Schedules, Dependencies, and Maintenance Window.

Access Rights

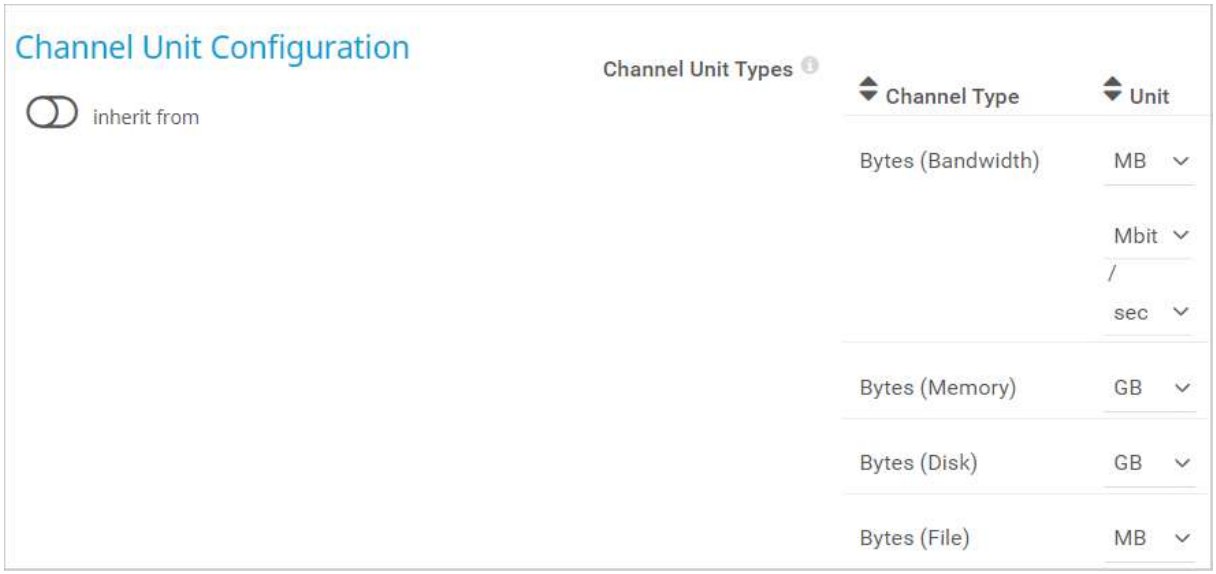


Access Rights

For more information, see section Root Group Settings, section Access Rights.

Channel Unit Configuration

Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.



Channel Unit Configuration

For more information, see section Root Group Settings, section Channel Unit Configuration.

Channel List

Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Alarm State	The alarm status This channel is the primary channel by default.
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
[Metric]	The metric on which the alarm is based

More

KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

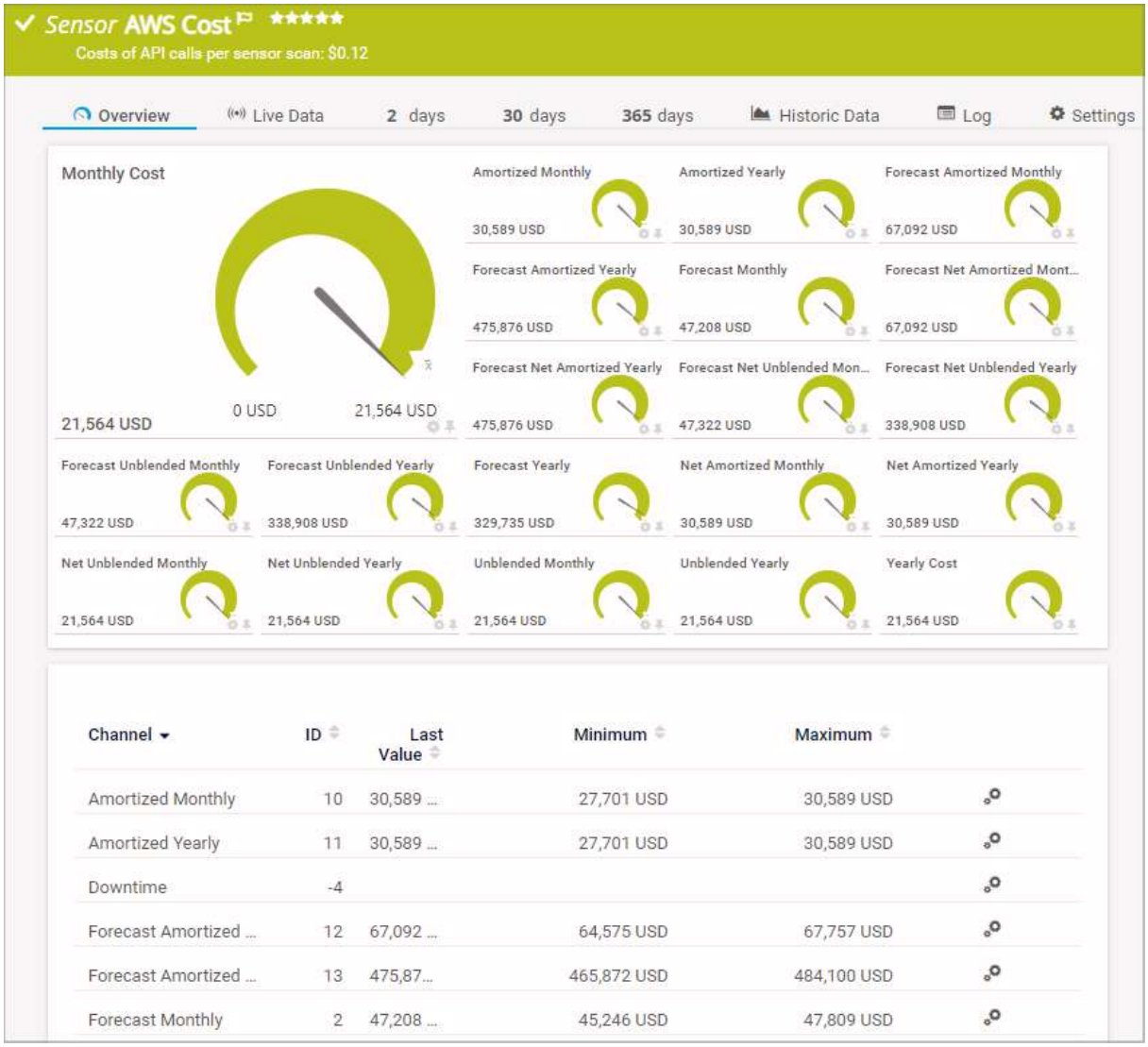
- https://kb.paessler.com/en/topic/38083

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

7.8.4 AWS Cost Sensor

The AWS Cost sensor monitors the cost of an Amazon Web Services (AWS) account by reading its data from the AWS Cost Explorer API.



AWS Cost Sensor

For a detailed list and descriptions of the channels that this sensor can show, see section Channel List 690.

Sensor in Other Languages

- Dutch: AWS Cost
- French: AWS Cost
- German: AWS Cost
- Japanese: AWS Cost
- Portuguese: AWS Cost
- Russian: AWS Cost

- Simplified Chinese: AWS Cost
- Spanish: AWS Cost

Remarks

- This sensor requires the AWS Cost Explorer to be activated in your AWS account.
- This sensor requires IAM User and Role Access to Billing Information to be enabled in your AWS account.
- This sensor requires 684 permissions for the AWS API key.
- This sensor requires credentials for AWS in settings that are higher in the object hierarchy.
- This sensor supports IPv6.
- This sensor has a low performance impact.
- After sensor creation, the first data is available after 24 hours. Forecast data is available after a few days.
- The recommended scanning interval for this sensor is 6 hours. You can use a shorter scanning interval but it could create extra costs.
- Amazon charges you for each API call that the sensor sends to the Amazon servers. For more information, see AWS Cost Management Pricing | Amazon Simple Storage Service.
- You can only set up this sensor for one AWS account per PRTG installation.
- Knowledge Base: What settings do I have to define in my AWS account to set up the AWS Cost sensor?
- Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

Detailed Requirements

Requirement	Description
Permissions for the AWS API key	This sensor requires sufficient rights to query data from the AWS API The AWS API key requires the following permissions: ▪ "ce:GetCostAndUsage" ▪ "ce:GetCostForecast" ▪ "ce:GetDimensionValues" ▪ "ce:GetCostAndUsageWithResources" ▪ "ce:GetUsageForecast" For more information, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

Basic Sensor Settings

Basic Sensor Settings

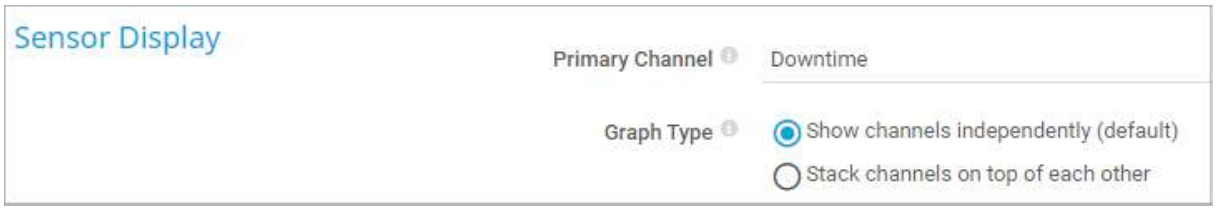
Setting	Description
Sensor Name	Enter a name to identify the sensor. By default, PRTG shows this name in the device tree, as well as in alarms, logs, notifications, reports, maps, libraries, and tickets. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Parent Tags	The tags that the sensor inherits from its parent device, parent group, and parent probe. ⓘ This setting is for your information only. You cannot change it.
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically inherited. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added. The sensor has the following default tags that are automatically predefined in the sensor's settings when you add the sensor: ▪ aws ▪ cost ▪ awscost
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

AWS Cost Specific

AWS Cost Specific

Setting	Description
Additional Cost Types	PRTG creates two default channels for blended monthly and yearly cost. If you select this option, you can select additional cost types for which PRTG creates additional channels.
Select Additional Cost Types	This setting is only visible if you select Enable for Additional Cost Types above. Select additional cost types: ▪ Amortized cost ▪ Net amortized cost ▪ Unblended cost ▪ Net unblended cost ⓘ PRTG creates two overview channels (monthly and yearly) for every additional cost type that you select.
Additional Forecast Types	PRTG does not automatically create additional forecast channels. If you select this option, you can select additional forecast types to create additional forecast channels.
Select Additional Forecast Types	This setting is only visible if you select Enable for Additional Cost Types above. Select additional forecast types: ▪ Blended cost (default) ▪ Amortized cost ▪ Net amortized cost ▪ Unblended cost ▪ Net unblended cost ⓘ PRTG creates two overview channels (monthly and yearly) for every additional forecast type that you select. Every forecast type that you select creates additional fees. Deselect a forecast type if you no longer want the according channels to create additional fees. You can still see the channels, but they do not receive data anymore.

Sensor Display



Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel is always displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set a different primary channel later by clicking 📌 below a channel gauge on the sensor's Overview tab.
Graph Type	Define how different channels are shown for this sensor: ▪ Show channels independently (default): Show a graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings).
Stack Unit	This setting is only visible if you enable Stack channels on top of each other as Graph Type. Select a unit from the list. All channels with this unit are stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Debug Options

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result:

Setting	Description
	▪ Discard result: Do not store the sensor result. ▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the PRTG data directory on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval. This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance. In a cluster, PRTG stores the result in the PRTG data directory of the master node.

Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

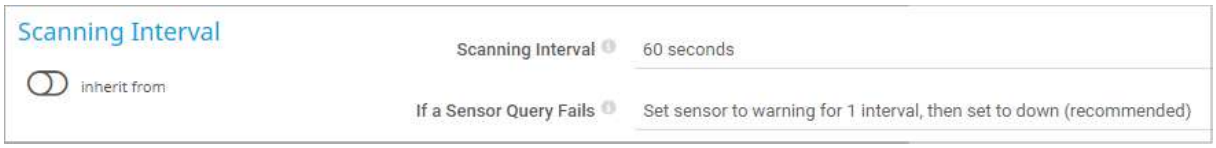
For more information, see section Inheritance of Settings.

Scanning Interval

This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the Monitoring settings are not available for this sensor.

The minimum scanning interval of this sensor is 1 hour.

The recommended scanning interval of this sensor is 6 hours.

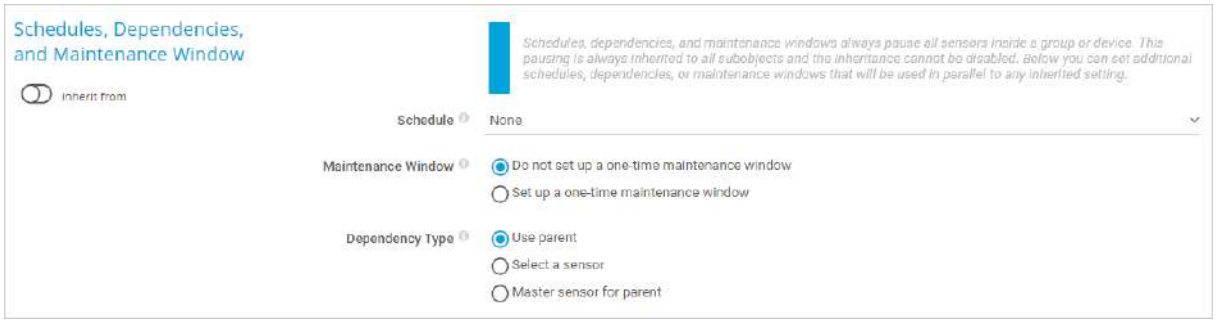


Scanning Interval

For more information, see section Root Group Settings, section Scanning Interval.

Schedules, Dependencies, and Maintenance Window

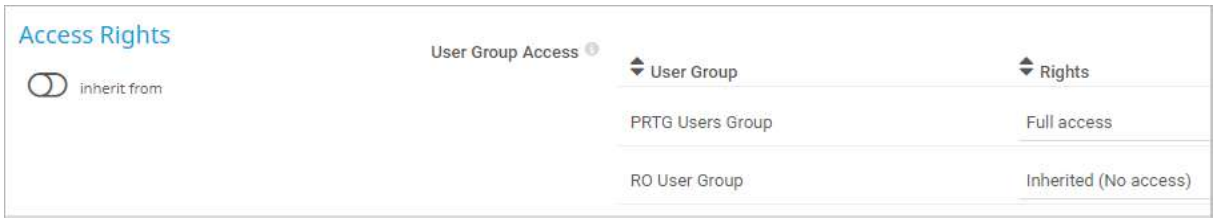
You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.



Schedules, Dependencies, and Maintenance Window

For more information, see section Root Group Settings, section Schedules, Dependencies, and Maintenance Window.

Access Rights

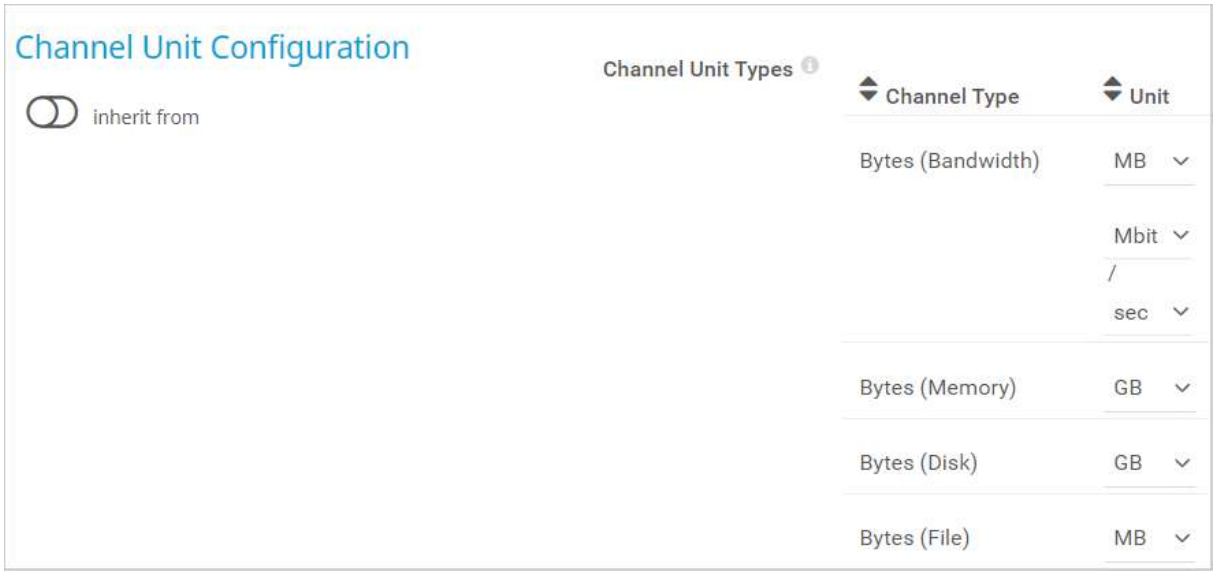


Access Rights

For more information, see section Root Group Settings, section Access Rights.

Channel Unit Configuration

Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.



Channel Unit Configuration

For more information, see section Root Group Settings, section Channel Unit Configuration.

Channel List

ⓘ Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Amortized Monthly	The amortized cost per month
Amortized Yearly	The amortized cost per year
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Forecast Amortized Monthly	The forecast for amortized cost per month
Forecast Amortized Yearly	The forecast for amortized cost per year
Forecast Monthly	The forecast for cost per month
Forecast Net Amortized Monthly	The forecast for net amortized cost per month
Forecast Net Amortized Yearly	The forecast for net amortized cost per year
Forecast Net Unblended Monthly	The forecast for net unblended cost per month
Forecast Net Unblended Yearly	The forecast for net unblended cost per year
Forecast Unblended Monthly	The forecast for unblended cost per month
Forecast Unblended Yearly	The forecast for unblended cost per year
Forecast Yearly	The forecast for cost per year
Monthly Cost	The monthly cost ⓘ This channel is the primary channel by default.

Channel	Description
Net Amortized Monthly	The net amortized cost per month
Net Amortized Yearly	The net amortized cost per year
Net Unblended Monthly	The net unblended cost per month
Net Unblended Yearly	The net unblended cost per year
Unblended Monthly	The unblended cost per month
Unblended Yearly	The unblended cost per year
Yearly Cost	The cost per year

More

KNOWLEDGE BASE

What settings do I have to define in my AWS account to set up the AWS Cost sensor?

- https://kb.paessler.com/en/topic/87401

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- https://kb.paessler.com/en/topic/38083

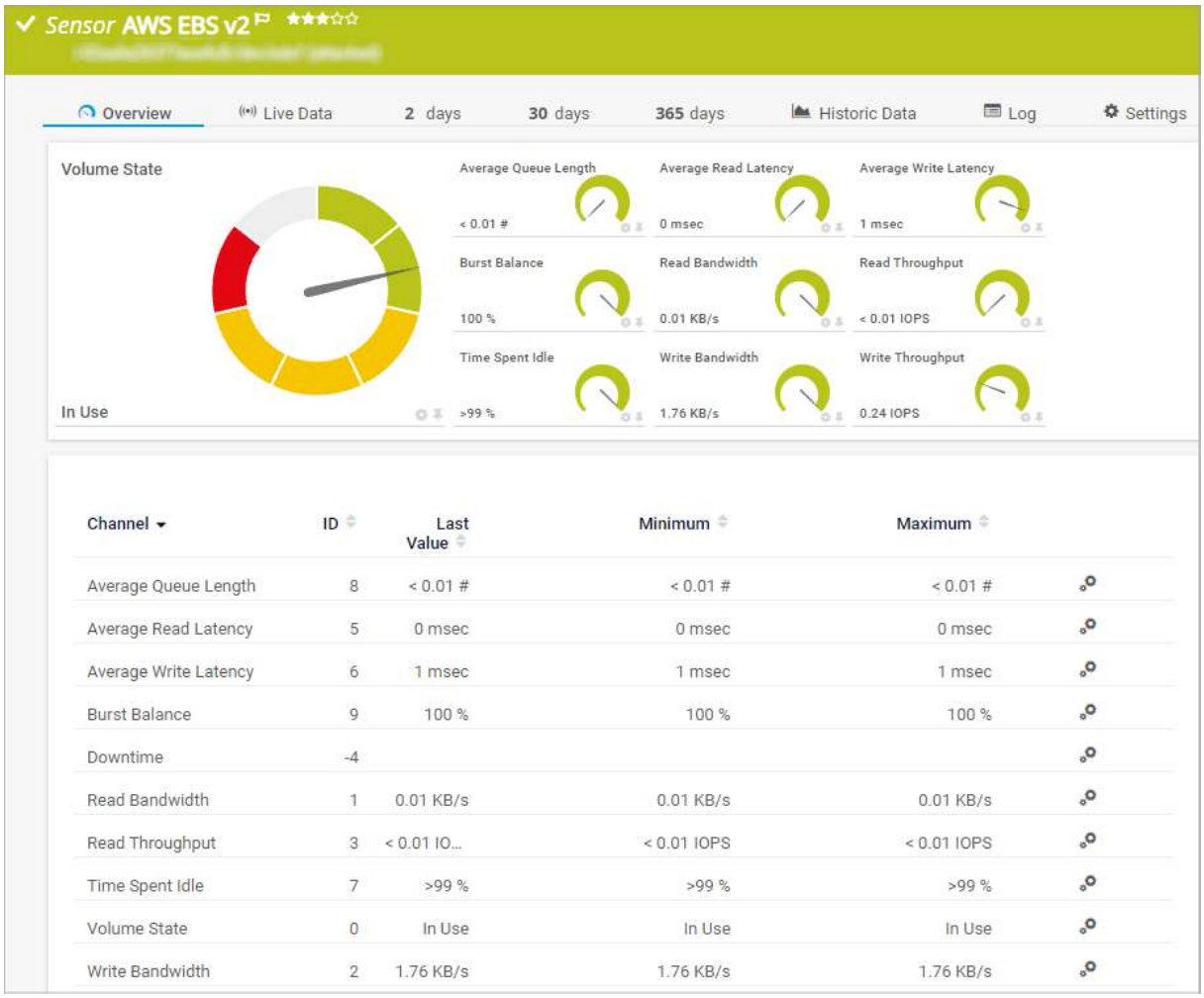
What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108

7.8.5 AWS EBS v2 Sensor

The AWS EBS v2 sensor monitors the performance of an Amazon Web Services (AWS) Elastic Block Store (EBS) volume by reading its data from Amazon CloudWatch via the AWS API.

ⓘ If you use the same Identity and Access Management (IAM) policy that you use for this sensor, you must update it. For more information, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?



Channel	ID	Last Value	Minimum	Maximum
Average Queue Length	8	< 0.01 #	< 0.01 #	< 0.01 #
Average Read Latency	5	0 msec	0 msec	0 msec
Average Write Latency	6	1 msec	1 msec	1 msec
Burst Balance	9	100 %	100 %	100 %
Downtime	-4			
Read Bandwidth	1	0.01 KB/s	0.01 KB/s	0.01 KB/s
Read Throughput	3	< 0.01 IO...	< 0.01 IOPS	< 0.01 IOPS
Time Spent Idle	7	>99 %	>99 %	>99 %
Volume State	0	In Use	In Use	In Use
Write Bandwidth	2	1.76 KB/s	1.76 KB/s	1.76 KB/s

AWS EBS v2 Sensor

- For a list of metrics that this sensor supports, see section Supported Metrics 698.
- For a list of dimensions that this sensor supports, see section Supported Dimensions 699.
- For a list of regions that this sensor supports, see section List of Supported AWS Regions and Their Codes.
- For a detailed list and descriptions of the channels that this sensor can show, see section Channel List 699.

Sensor in Other Languages

- Dutch: AWS EBS v2
- French: AWS EBS v2
- German: AWS EBS v2
- Japanese: AWS EBS v2
- Portuguese: AWS EBS v2
- Russian: AWS EBS v2
- Simplified Chinese: AWS EBS v2
- Spanish: AWS EBS v2

Remarks

- This sensor requires 693 permissions for the AWS API key.
- This sensor requires credentials for AWS in settings that are higher in the object hierarchy.
- This sensor supports IPv6.
- This sensor has a low performance impact.
- This sensor uses lookups to determine the status values of one or more channels.
- Amazon can charge you based on the number of API calls that the sensor sends to the Amazon servers. For more information, see Amazon CloudWatch Pricing – Amazon Web Services (AWS).
- It can take up to several minutes before objects appear in the Add Sensor dialog.

Detailed Requirements

Requirement	Description
Permissions for the AWS API key	This sensor requires sufficient rights to query data from the AWS API For more information, see the Knowledge Base: How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

Basic Sensor Settings

Basic Sensor Settings

Setting	Description
Sensor Name	Enter a name to identify the sensor. By default, PRTG shows this name in the device tree, as well as in alarms, logs, notifications, reports, maps, libraries, and tickets. ⓘ If the name contains angle brackets (<>), PRTG replaces them with braces ({}) for security reasons. For more information, see the Knowledge Base: What security features does PRTG include?
Parent Tags	The tags that the sensor inherits from its parent device, parent group, and parent probe. ⓘ This setting is for your information only. You cannot change it.
Tags	Enter one or more tags. Confirm each tag with the Spacebar key, a comma, or the Enter key. You can use tags to group objects and use tag-filtered views later on. Tags are not case-sensitive. Tags are automatically inherited. ⓘ It is not possible to enter tags with a leading plus (+) or minus (-) sign, nor tags with parentheses (()) or angle brackets (<>). ⓘ For performance reasons, it can take some minutes until you can filter for new tags that you added. The sensor has the following default tags that are automatically predefined in the sensor's settings when you add the sensor: ▪ aws ▪ cloudwatch ▪ cloudwatchsensor ▪ ebs

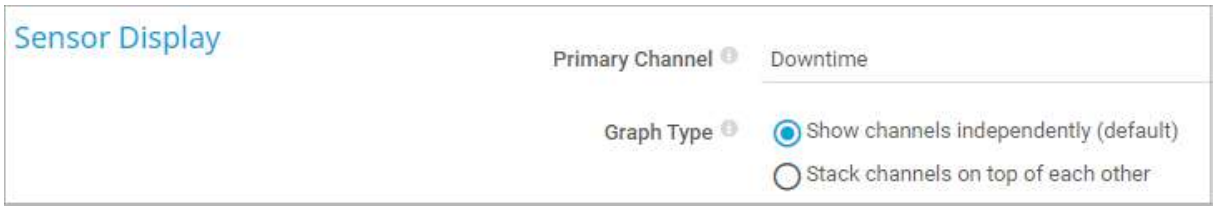
Setting	Description
Priority	Select a priority for the sensor. This setting determines the position of the sensor in lists. The highest priority is at the top of a list. Choose from the lowest priority (★☆☆☆☆) to the highest priority (★★★★★).

AWS EBS Specific

AWS EBS Specific

Setting	Description
ID	The ID of the AWS EBS volume that this sensor monitors.
Name	The name of the AWS EBS volume that this sensor monitors.
Region	The region in which the AWS EBS instance runs. For a list of regions that this sensor supports, see section List of Supported AWS Regions and Their Codes.

Sensor Display



Sensor Display

Setting	Description
Primary Channel	Select a channel from the list to define it as the primary channel. In the device tree, the last value of the primary channel is always displayed below the sensor's name. The available options depend on what channels are available for this sensor. ⓘ You can set a different primary channel later by clicking 📌 below a channel gauge on the sensor's Overview tab.
Graph Type	Define how different channels are shown for this sensor: ▪ Show channels independently (default): Show a graph for each channel. ▪ Stack channels on top of each other: Stack channels on top of each other to create a multi-channel graph. This generates a graph that visualizes the different components of your total traffic. ⓘ You cannot use this option in combination with manual Vertical Axis Scaling (available in the channel settings).
Stack Unit	This setting is only visible if you enable Stack channels on top of each other as Graph Type. Select a unit from the list. All channels with this unit are stacked on top of each other. By default, you cannot exclude single channels from stacking if they use the selected unit. However, there is an advanced procedure to do so.

Debug Options

Debug Options

Setting	Description
Result Handling	Define what PRTG does with the sensor result: ▪ Discard result: Do not store the sensor result. ▪ Store result: Store the last sensor result in the \Logs\sensors subfolder of the PRTG data directory on the probe system. The file name is Result of Sensor [ID].log. This setting is for debugging purposes. PRTG overwrites this file with each scanning interval. ☁ This option is not available when the sensor runs on the hosted probe of a PRTG Hosted Monitor instance. ⓘ In a cluster, PRTG stores the result in the PRTG data directory of the master node.

Inherited Settings

By default, all of these settings are inherited from objects that are higher in the hierarchy. We recommend that you change them centrally in the root group settings if necessary. To change a setting for this object only, click under the corresponding setting name to disable the inheritance and to display its options.

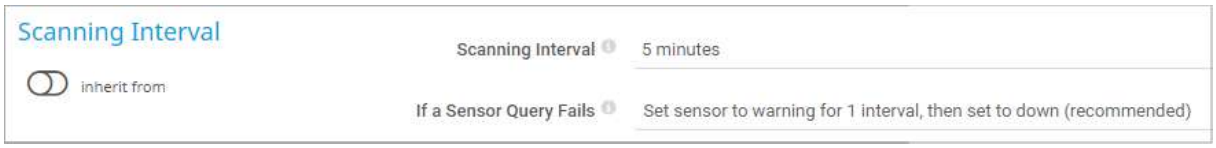
For more information, see section Inheritance of Settings.

Scanning Interval

This sensor has a fixed minimum scanning interval for performance reasons. You cannot use a shorter scanning interval. Consequently, shorter scanning intervals in the Monitoring settings are not available for this sensor.

The minimum scanning interval of this sensor is 1 minute.

The recommended scanning interval of this sensor is 5 minutes.

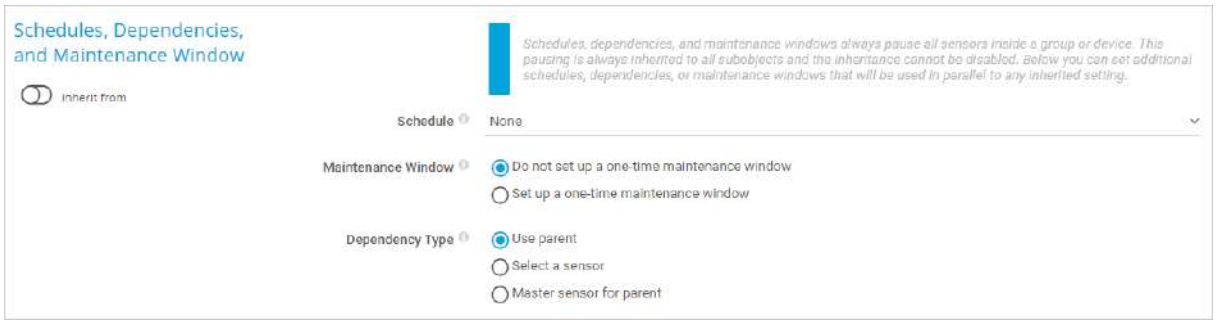


Scanning Interval

For more information, see section Root Group Settings, section Scanning Interval.

Schedules, Dependencies, and Maintenance Window

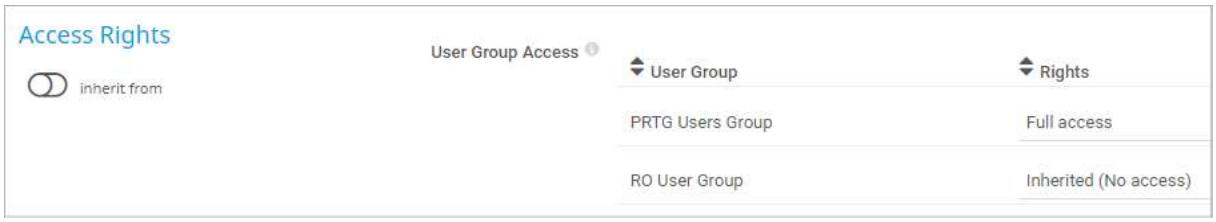
You cannot interrupt the inheritance for schedules, dependencies, and maintenance windows. The corresponding settings from the parent objects are always active. However, you can define additional schedules, dependencies, and maintenance windows. They are active at the same time as the parent objects' settings.



Schedules, Dependencies, and Maintenance Window

For more information, see section Root Group Settings, section Schedules, Dependencies, and Maintenance Window.

Access Rights

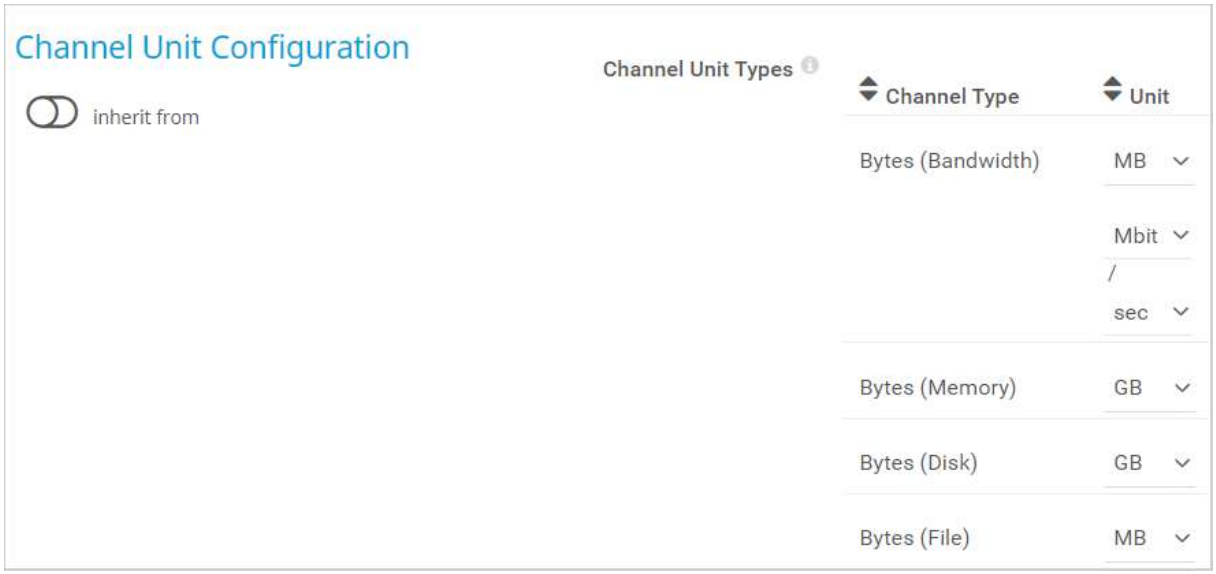


Access Rights

For more information, see section Root Group Settings, section Access Rights.

Channel Unit Configuration

Which channel units are available depends on the sensor type and the available parameters. If no configurable channels are available, this field shows No configurable channels.



Channel Unit Configuration

For more information, see section Root Group Settings, section Channel Unit Configuration.

Supported Metrics

The AWS EBS v2 sensor supports the following metrics:

- BurstBalance (Average)
- VolumeIdleTime (Sum)
- VolumeQueueLength (Average)
- VolumeReadBytes (Sum)
- VolumeReadOps (Sum)
- VolumeTotalReadTime (Average)
- VolumeTotalWriteTime (Average)

- VolumeWriteBytes (Sum)
- VolumeWriteOps (Sum)

Supported Dimensions

The AWS EBS v2 sensor supports the following dimensions:

- Volume

Channel List

Which channels the sensor actually shows might depend on the target device, the available components, and the sensor setup.

Channel	Description
Average Queue Length	The average queue lengths
Average Read Latency	The average read latency
Average Write Latency	The average write latency
Burst Balance	The burst balance
Downtime	In the channel table on the Overview tab, this channel never shows any values. PRTG uses this channel in graphs and reports to show the amount of time in which the sensor was in the Down status
Read Bandwidth	The read bandwidth
Read Throughput	The read throughput in IOPS
Time Spent Idle	The time spent idle (%)
Volume State	The volume status ▪ Up status: Available, In Use ▪ Warning status: Creating, Deleting, Deleted ▪ Down status: Error ▪ Unknown status: Not Set This channel is the primary channel by default.
Write Bandwidth	The write bandwidth

Channel	Description
Write Throughput	The write throughput in IOPS

More

KNOWLEDGE BASE

How do I set permissions for the Amazon Web Services (AWS) API key to use certain sensors in PRTG?

- https://kb.paessler.com/en/topic/38083

What security features does PRTG include?

- https://kb.paessler.com/en/topic/61108