Use SNMP monitoring

StorageGRID 11.7

NetApp
January 09, 2024

Table of Contents

Use SNMP monitoring

Use SNMP monitoring: Overview

If you want to monitor StorageGRID using the Simple Network Management Protocol (SNMP), you must configure the SNMP agent that is included with StorageGRID.

- Configure the SNMP agent
- Update the SNMP agent

Capabilities

Each StorageGRID node runs an SNMP agent, or daemon, that provides a MIB. The StorageGRID MIB contains table and notification definitions for alerts and alarms. The MIB also contains system description information such as platform and model number for each node. Each StorageGRID node also supports a subset of MIB-II objects.

See Access MIB files if you want to download the MIB files on your grid nodes.

Initially, SNMP is disabled on all nodes. When you configure the SNMP agent, all StorageGRID nodes receive the same configuration.

The StorageGRID SNMP agent supports all three versions of the SNMP protocol. It provides read-only MIB access for queries, and it can send two types of event-driven notifications to a management system:

- **Traps** are notifications sent by the SNMP agent that don't require acknowledgment by the management system. Traps serve to notify the management system that something has happened within StorageGRID, such as an alert being triggered.

  Traps are supported in all three versions of SNMP.

- **Informs** are similar to traps, but they require acknowledgment by the management system. If the SNMP agent does not receive an acknowledgment within a certain amount of time, it resends the inform until an acknowledgment is received or the maximum retry value has been reached.

  Informs are supported in SNMPv2c and SNMPv3.

Trap and inform notifications are sent in the following cases:

- A default or custom alert is triggered at any severity level. To suppress SNMP notifications for an alert, you must configure a silence for the alert. Alert notifications are sent by the preferred sender Admin Node.

  Each alert is mapped to one of three trap types based on the severity level of the alert: activeMinorAlert, activeMajorAlert, and activeCriticalAlert. For a list of the alerts that can trigger these traps, see the Alerts reference.

- Certain alarms (legacy system) are triggered at specified severity levels or higher.

  SNMP notifications aren't sent for every alarm or every alarm severity.

SNMP version support

The table provides a high-level summary of what is supported for each SNMP version.

	SNMPv1	SNMPv2c	SNMPv3
Queries	Read-only MIB queries	Read-only MIB queries	Read-only MIB queries
Query authentication	Community string	Community string	User-based Security Model (USM) user
Notifications	Traps only	Traps and informs	Traps and informs
Notification authentication	Default trap community or a custom community string for each trap destination	Default trap community or a custom community string for each trap destination	USM user for each trap destination

Limitations

- StorageGRID supports read-only MIB access. Read-write access is not supported.
- All nodes in the grid receive the same configuration.
- SNMPv3: StorageGRID does not support the Transport Support Mode (TSM).
- SNMPv3: The only authentication protocol supported is SHA (HMAC-SHA-96).
- SNMPv3: The only privacy protocol supported is AES.

Related information

- Alerts reference
- Alarms reference (legacy system)
- Silence alert notifications

Configure the SNMP agent

You can configure the StorageGRID SNMP agent if you want to use a third-party SNMP management system for read-only MIB access and notifications.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.

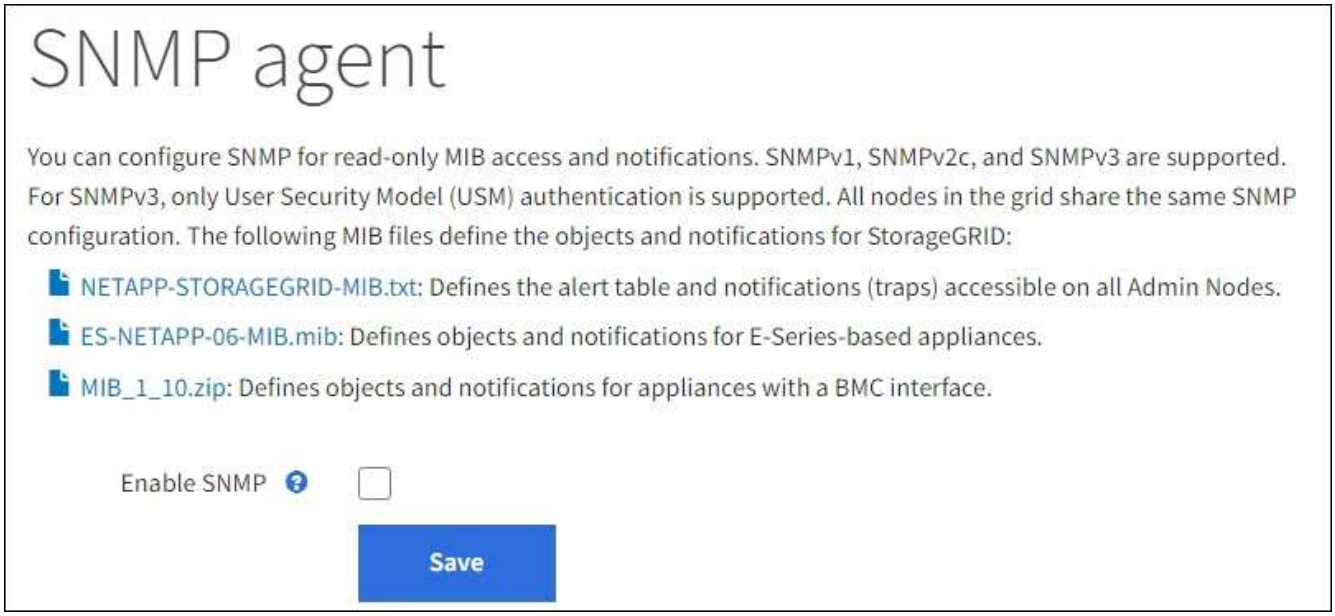
About this task

The StorageGRID SNMP agent supports all three versions of the SNMP protocol. You can configure the agent for one or more versions.

Steps

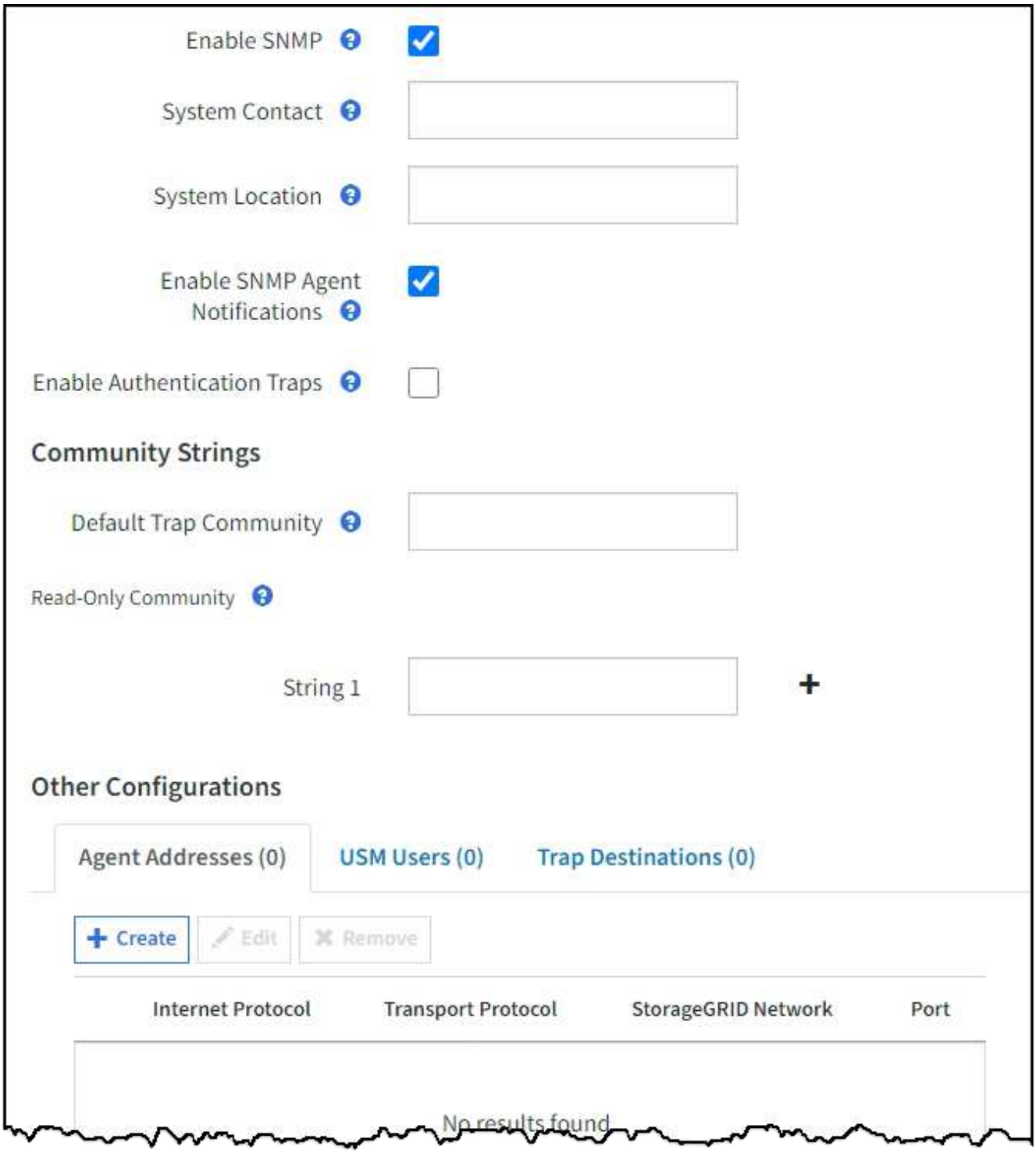
1. Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.

   The SNMP Agent page appears.



2. To enable the SNMP agent on all grid nodes, select the **Enable SNMP** checkbox.

   The fields for configuring an SNMP agent appear.



3. In the **System Contact** field, enter the value you want StorageGRID to provide in SNMP messages for sysContact.

   The System Contact typically is an email address. The value you provide applies to all nodes in the StorageGRID system. **System Contact** can be a maximum of 255 characters.

4. In the **System Location** field, enter the value you want StorageGRID to provide in SNMP messages for sysLocation.

   The System Location can be any information that is useful for identifying where your StorageGRID system is located. For example, you might use the street address of a facility. The value you provide applies to all

nodes in the StorageGRID system. **System Location** can be a maximum of 255 characters.

5. Keep the **Enable SNMP Agent Notifications** checkbox selected if you want the StorageGRID SNMP agent to send trap and inform notifications.

   If this checkbox is cleared, the SNMP agent supports read-only MIB access, but it does not send any SNMP notifications.

6. Select the **Enable Authentication Traps** checkbox if you want the StorageGRID SNMP agent to send an authentication trap if it receives an improperly authenticated protocol message.
7. If you use SNMPv1 or SNMPv2c, complete the Community Strings section.

   The fields in this section are used for community-based authentication in SNMPv1 or SNMPv2c. These fields don't apply to SNMPv3.

   a. In the **Default Trap Community** field, optionally enter the default community string you want to use for trap destinations.

      As required, you can provide a different ("custom") community string when you define a specific trap destination.

      Default Trap Community can be a maximum of 32 characters and can't contain whitespace characters.

   b. For **Read-Only Community**, enter one or more community strings to allow read-only MIB access on IPv4 and IPv6 agent addresses. Select the plus sign ➕ to add multiple strings.

      When the management system queries the StorageGRID MIB, it sends a community string. If the community string matches one of the values specified here, the SNMP agent sends a response to the management system.

      Each community string can be a maximum of 32 characters and can't contain whitespace characters. Up to five strings are allowed.

      > ⓘ To ensure the security of your StorageGRID system, don't use "public" as the community string. If you don't enter a community string, the SNMP agent uses the grid ID of your StorageGRID system as the community string.

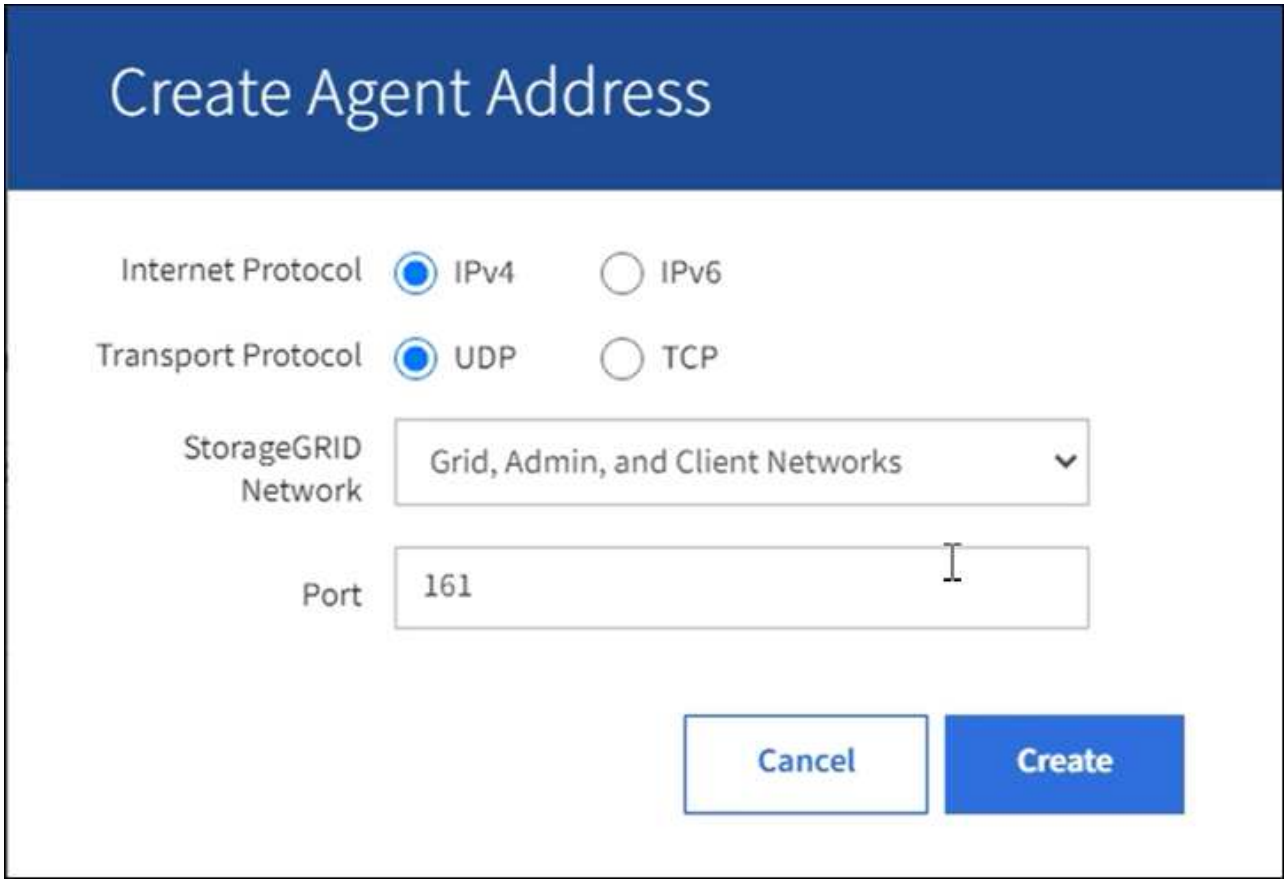
8. Optionally, select the Agent Addresses tab in the Other Configurations section.

   Use this tab to specify one or more "listening addresses." These are the StorageGRID addresses on which the SNMP agent can receive queries. Each agent address includes an internet protocol, a transport protocol, a StorageGRID network, and optionally a port.

   If you don't configure an agent address, the default listening address is UDP port 161 on all StorageGRID networks.

   a. Select **Create**.

      The Create Agent Address dialog box appears.



b. For **Internet Protocol**, select whether this address will use IPv4 or IPv6.

   By default, SNMP uses IPv4.

c. For **Transport Protocol**, select whether this address will use UDP or TCP.

   By default, SNMP uses UDP.

d. In the **StorageGRID Network** field, select which StorageGRID network the query will be received on.

   - Grid, Admin, and Client Networks: StorageGRID should listen for SNMP queries on all three networks.
   - Grid Network
   - Admin Network
   - Client Network

   > To ensure that client communications with StorageGRID remain secure, you should not create an agent address for the Client Network.

e. In the **Port** field, optionally enter the port number that the SNMP agent should listen on.

   The default UDP port for an SNMP agent is 161, but you can enter any unused port number.

   > When you save the SNMP agent, StorageGRID automatically opens the agent address ports on the internal firewall. You must ensure that any external firewalls allow access to these ports.

f. Select **Create**.

The agent address is created and added to the table.

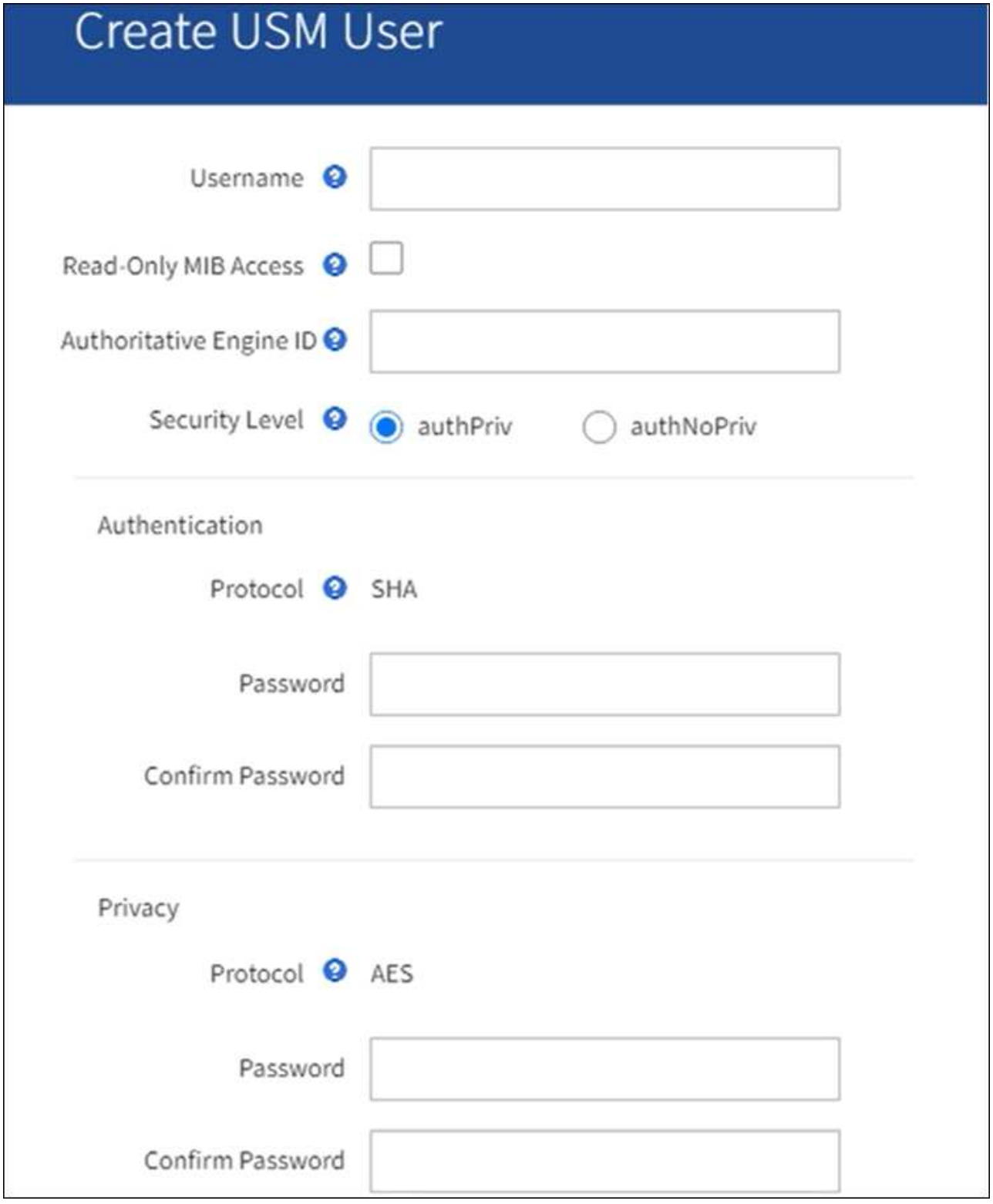
9. If you are using SNMPv3, select the USM Users tab in the Other Configurations section.

Use this tab to define the USM users who are authorized to query the MIB or to receive traps and informs.

This step does not apply if you are only using SNMPv1 or SNMPv2c.

a. Select **Create**.

The Create USM User dialog box appears.



b. Enter a unique **Username** for this USM user.

   Usernames have a maximum of 32 characters and can't contain whitespace characters. The username can't be changed after the user is created.

c. Select the **Read-Only MIB Access** checkbox if this user should have read-only access to the MIB.

   If you select **Read-Only MIB Access**, the **Authoritative Engine ID** field is disabled.

USM users who have read-only MIB access can't have engine IDs.

d. If this user will be used in an inform destination, enter the **Authoritative Engine ID** for this user.

SNMPv3 inform destinations must have users with engine IDs. SNMPv3 trap destination can't have users with engine IDs.

The authoritative engine ID can be from 5 to 32 bytes in hexadecimal.

e. Select a security level for the USM user.

- **authPriv**: This user communicates with authentication and privacy (encryption). You must specify an authentication protocol and password and a privacy protocol and password.
- **authNoPriv**: This user communicates with authentication and without privacy (no encryption). You must specify an authentication protocol and password.

f. Enter and confirm the password this user will use for authentication.

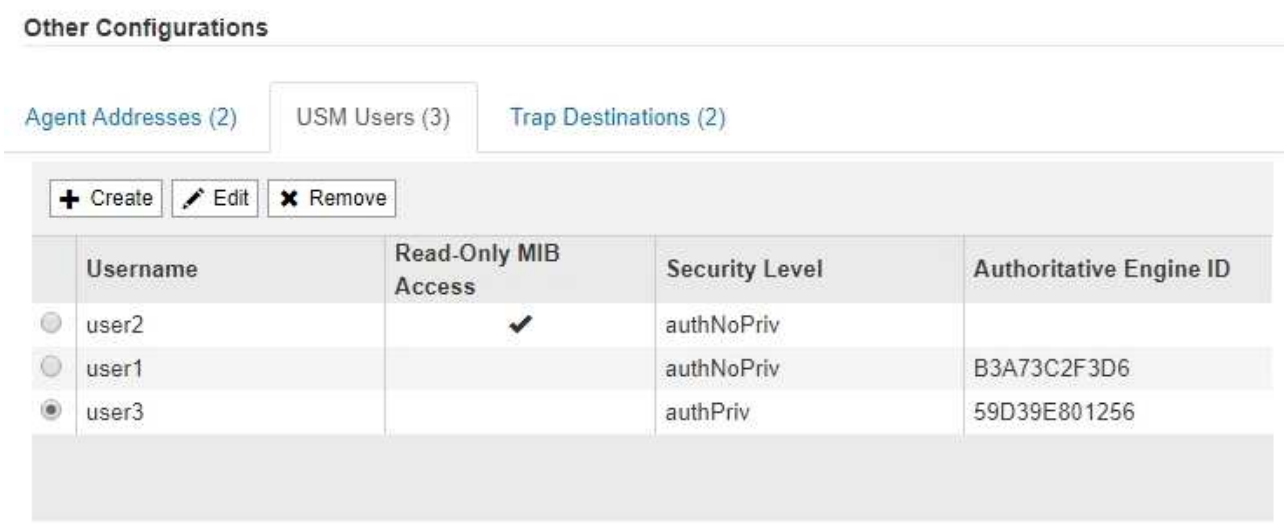
The only authentication protocol supported is SHA (HMAC-SHA-96).

g. If you selected **authPriv**, enter and confirm the password this user will use for privacy.

The only privacy protocol supported is AES.

h. Select **Create**.

The USM user is created and added to the table.

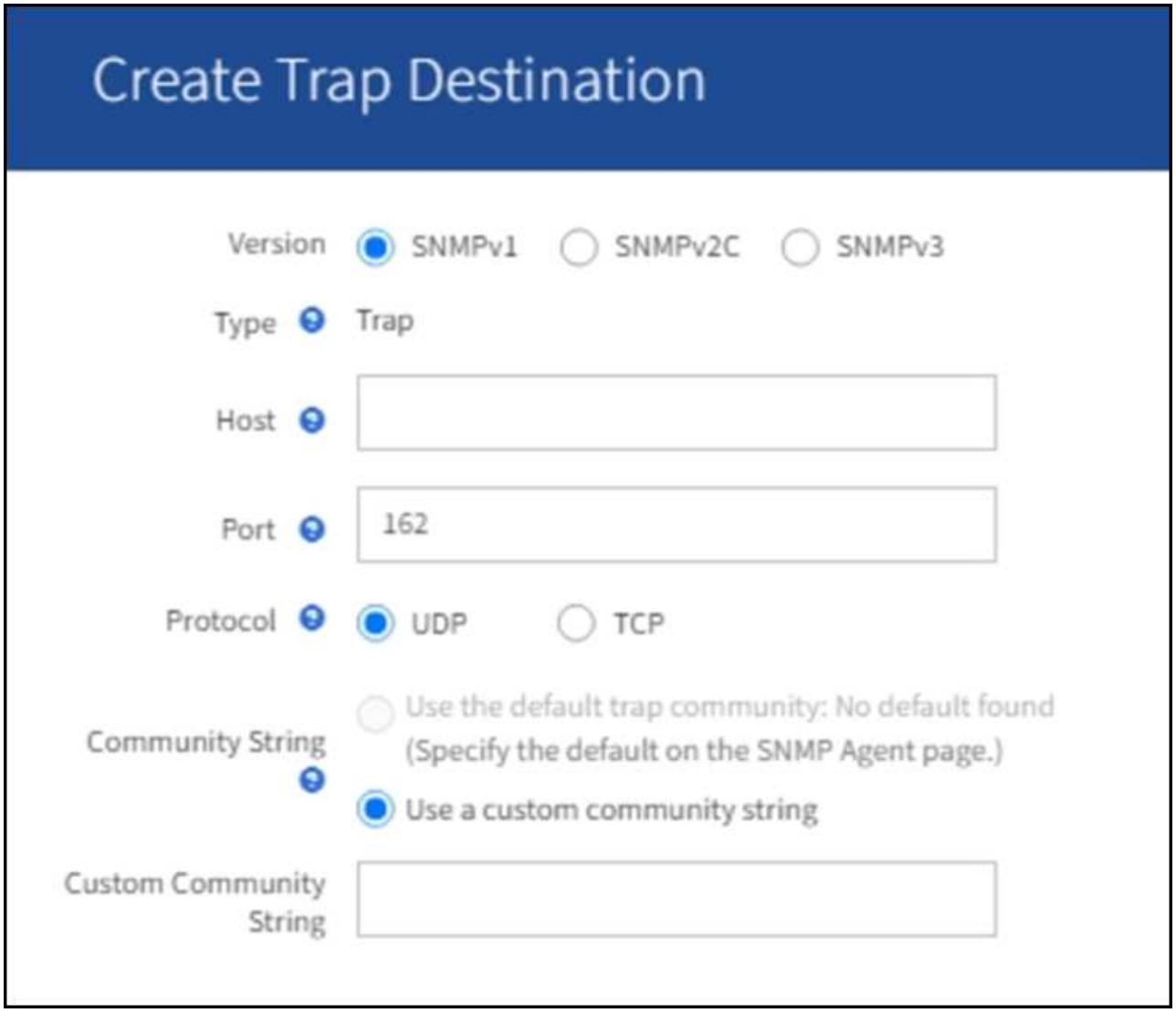


10. In the Other Configurations section, select the Trap Destinations tab.

The Trap Destinations tab allows you to define one or more destinations for StorageGRID trap or inform notifications. When you enable the SNMP agent and select **Save**, StorageGRID starts sending notifications to each defined destination. Notifications are sent when alerts are triggered. Standard notifications are also sent for the supported MIB-II entities (for example, ifDown and coldStart).

a. Select **Create**.

The Create Trap Destination dialog box appears.



b. In the **Version** field, select which SNMP version will be used for this notification.

c. Complete the form, based on which version you selected

Version	Specify this information
SNMPv1 (For SNMPv1, the SNMP agent can only send traps. Informs aren't supported.)	1. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap. 2. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.) 3. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.) 4. Use the default trap community, if one was specified on the SNMP Agent page, or enter a custom community string for this trap destination. The custom community string can be a maximum of 32 characters and can't contain whitespace.

Version	Specify this information
SNMPv2c	1. Select whether the destination will be used for traps or informs. 2. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap. 3. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.) 4. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.) 5. Use the default trap community, if one was specified on the SNMP Agent page, or enter a custom community string for this trap destination. The custom community string can be a maximum of 32 characters and can't contain whitespace.
SNMPv3	1. Select whether the destination will be used for traps or informs. 2. In the **Host** field, enter an IPv4 or IPv6 address (or FQDN) to receive the trap. 3. For **Port**, use the default (162), unless you must use another value. (162 is the standard port for SNMP traps.) 4. For **Protocol**, use the default (UDP). TCP is also supported. (UDP is the standard SNMP trap protocol.) 5. Select the USM user that will be used for authentication. ◦ If you selected **Trap**, only USM users without authoritative engine IDs are shown. ◦ If you selected **Inform**, only USM users with authoritative engine IDs are shown.

d. Select **Create**.

The trap destination is created and added to the table.

11. When you have completed the SNMP agent configuration, select **Save**.

The new SNMP agent configuration becomes active.

Related information

Silence alert notifications

Update the SNMP agent

You might want to disable SNMP notifications, update community strings, or add or remove agent addresses, USM users, and trap destinations.

Before you begin

- You must be signed in to the Grid Manager using a supported web browser.
- You must have the Root access permission.

About this task

Whenever you update the SNMP agent configuration, be aware that you must select **Save** at the bottom on the SNMP Agent page to commit any changes you have made on each tab.

Steps

1. Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.

   The SNMP Agent page appears.

2. If you want to disable the SNMP agent on all grid nodes, clear the **Enable SNMP** checkbox, and select **Save**.

   The SNMP agent is disabled for all grid nodes. If you later re-enable the agent, any previous SNMP configuration settings are retained.

3. Optionally, update the values you entered for **System Contact** and **System Location**.
4. Optionally, clear the **Enable SNMP Agent Notifications** checkbox if you no longer want the StorageGRID SNMP agent to send trap and inform notifications.

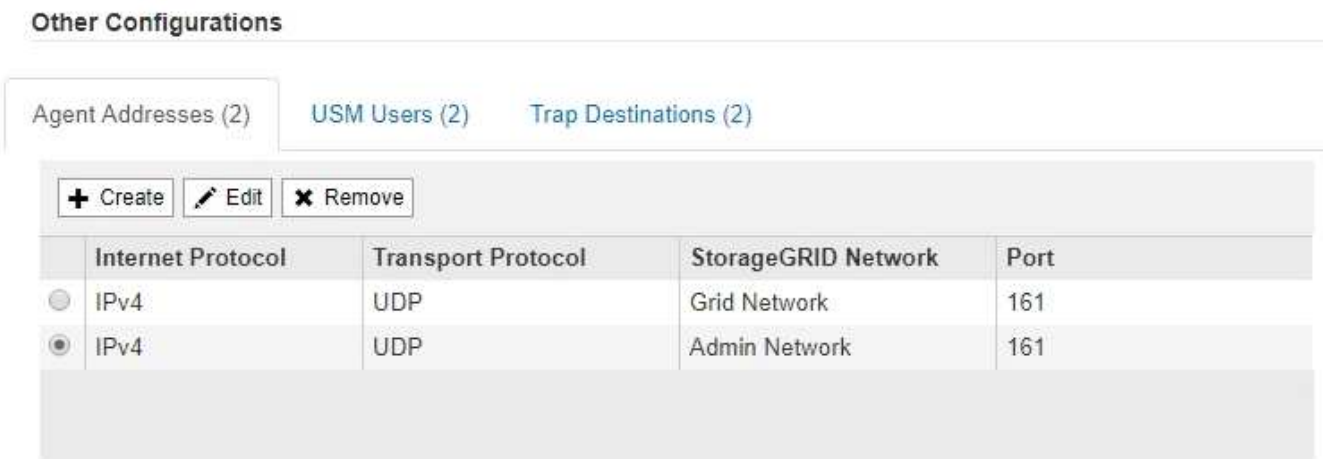
   When this checkbox is cleared, the SNMP agent supports read-only MIB access, but it does not send any SNMP notifications.

5. Optionally, clear the **Enable Authentication Traps** checkbox if you no longer want the StorageGRID SNMP agent to send an authentication trap when it receives an improperly authenticated protocol message.
6. If you use SNMPv1 or SNMPv2c, optionally update the Community Strings section.

   The fields in this section are used for community-based authentication in SNMPv1 or SNMPv2c. These fields don't apply to SNMPv3.

   If you want to remove the default community string, you must first ensure that all trap destinations use a custom community string.

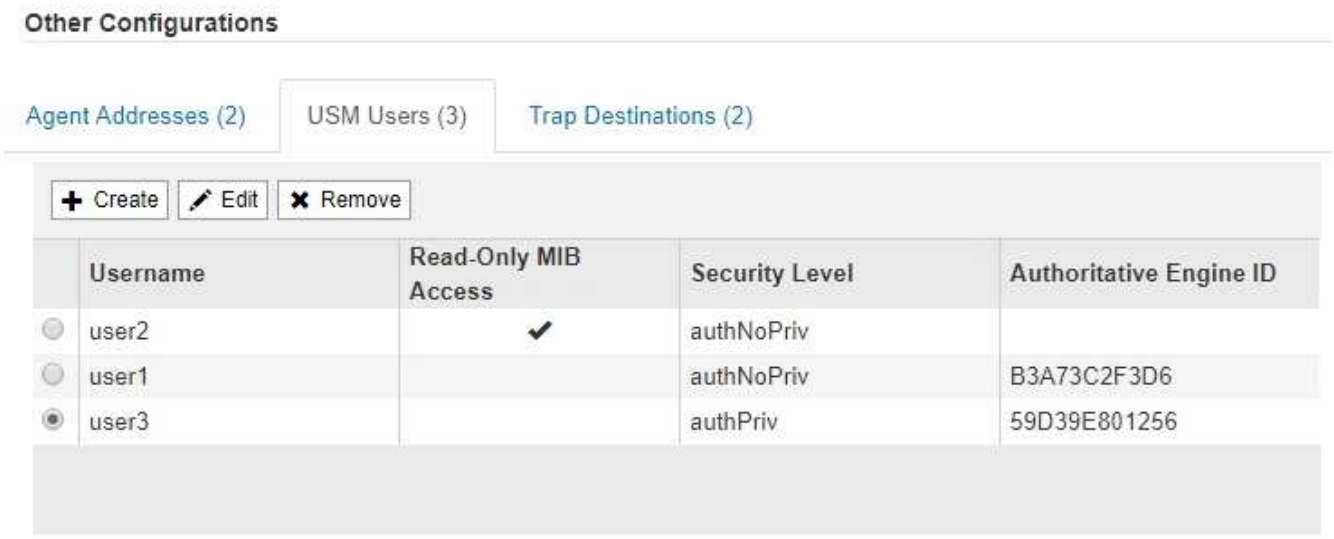
7. If you want to update agent addresses, select the Agent Addresses tab in the Other Configurations section.



Use this tab to specify one or more “listening addresses.” These are the StorageGRID addresses on which the SNMP agent can receive queries. Each agent address includes an internet protocol, a transport protocol, a StorageGRID network, and a port.

a. To add an agent address, select **Create**. Then, refer to the step for agent addresses in the instructions for configuring the SNMP agent.
b. To edit an agent address, select the radio button for the address, and select **Edit**. Then, refer to the step for agent addresses in the instructions for configuring the SNMP agent.
c. To remove an agent address, select the radio button for the address, and select **Remove**. Then, select **OK** to confirm that you want to remove this address.
d. To commit your changes, select **Save** at the bottom of the SNMP Agent page.

8. If you want to update USM users, select the USM Users tab in the Other Configurations section.



Use this tab to define the USM users who are authorized to query the MIB or to receive traps and informs.

a. To add a USM user, select **Create**. Then, refer to the step for USM users in the instructions for configuring the SNMP agent.
b. To edit a USM user, select the radio button for the user, and select **Edit**. Then, refer to the step for USM users in the instructions for configuring the SNMP agent.

   The username for an existing USM user can’t be changed. If you need to change a username, you must remove the user and create a new one.

   > If you add or remove a user’s authoritative engine ID and that user is currently selected for a destination, you must edit or remove the destination, as described in step SNMP trap destination. Otherwise, a validation error occurs when you save the SNMP agent configuration.

c. To remove a USM user, select the radio button for the user, and select **Remove**. Then, select **OK** to confirm that you want to remove this user.

   > If the user you removed is currently selected for a trap destination, you must edit or remove the destination, as described in step SNMP trap destination. Otherwise, a validation error occurs when you save the SNMP agent configuration.

d. To commit your changes, select **Save** at the bottom of the SNMP Agent page.

9. If you want to update trap destinations, select the Trap Destinations tab in the Other Configurations section.

   The Trap Destinations tab allows you to define one or more destinations for StorageGRID trap or inform notifications. When you enable the SNMP agent and select **Save**, StorageGRID starts sending notifications to each defined destination. Notifications are sent when alerts and alarms are triggered. Standard notifications are also sent for the supported MIB-II entities (for example, ifDown and coldStart).

   a. To add a trap destination, select **Create**. Then, refer to the step for trap destinations in the instructions for configuring the SNMP agent.

   b. To edit a trap destination, select the radio button for the user, and select **Edit**. Then, refer to the step for trap destinations in the instructions for configuring the SNMP agent.

   c. To remove a trap destination, select the radio button for the destination, and select **Remove**. Then, select **OK** to confirm that you want to remove this destination.

   d. To commit your changes, select **Save** at the bottom of the SNMP Agent page.

10. When you have updated the SNMP agent configuration, select **Save**.

Access MIB files

MIB files contain definitions and information about the properties of managed resources and services for the nodes in your grid. You can access MIB files that define the objects and notifications for StorageGRID. These files can be useful for monitoring your grid.

See Use SNMP monitoring for more information about SNMP and MIB files.

Access MIB files

Steps

1. Select **CONFIGURATION** > **Monitoring** > **SNMP agent**.
2. On the SNMP agent page, select the file you want to download:
   - **NETAPP-STORAGEGRID-MIB.txt**: Defines the alert table and notifications (traps) accessible on all Admin Nodes.
   - **ES-NETAPP-06-MIB.mib**: Defines objects and notifications for E-Series-based appliances.
   - **MIB_1_10.zip**: Defines objects and notifications for appliances with a BMC interface.
3. Optionally, you can access MIB files at the following location on any StorageGRID node: `/usr/share/snmp/mibs`
4. To extract the `storagegrid` OIDs from the MIB file:
   a. Get the OID of the root of the StorageGRID MIB:

      ```
      root@user-adm1:~ # snmptranslate -On -IR storagegrid
      ```

      Result: `.1.3.6.1.4.1.789.28669` (`28669` is always the OID for StorageGRID)

   b. Then grep for the StorageGRID OID in the entire tree (using paste to join lines):

      ```
      root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
      ```

The `snmptranslate` command has many options that are useful for exploring the MIB. This command is available on any StorageGRID node.

MIB file contents

All objects are under the storagegrid OID.

Object name	Object ID (OID)	Description
`.iso.org.dod.internet.private.enterprises.netapp.storagegrid`	`.1.3.6.1.4.1.789.28669`	The MIB Module for NetApp StorageGRID entities.

MIB Objects

Object Name	Object ID (OID)	Description
`activeAlertCount`	`.1.3.6.1.4.1.789.28669.1.3`	The number of active alerts in the activeAlertTable.
`activeAlertTable`	`.1.3.6.1.4.1.789.28669.1.4`	A table of active alerts in StorageGRID.
`activeAlertId`	`.1.3.6.1.4.1.789.28669.1.4.1.1`	The ID of the alert. Only unique in the current set of active alerts.
`activeAlertName`	`.1.3.6.1.4.1.789.28669.1.4.1.2`	The name of the alert.
`activeAlertInstance`	`.1.3.6.1.4.1.789.28669.1.4.1.3`	The name of the entity that generated the alert, typically the node name.
`activeAlertSeverity`	`.1.3.6.1.4.1.789.28669.1.4.1.4`	The severity of the alert.
`activeAlertStartTime`	`.1.3.6.1.4.1.789.28669.1.4.1.5`	Date and time the alert was triggered.

Notification Types (Traps)

All notifications include the following variables as varbinds:

- activeAlertId
- activeAlertName
- activeAlertInstance
- activeAlertSeverity
- activeAlertStartTime

Notification Type	Object ID (OID)	Description
activeMinorAlert	.1.3.6.1.4.1.789.28669.0.6	An alert with minor severity
activeMajorAlert	.1.3.6.1.4.1.789.28669.0.7	An alert with major severity
activeCriticalAlert	.1.3.6.1.4.1.789.28669.0.8	An alert with critical severity

Copyright information

Trademark information