SNMP

This chapter describes the Simple Network Management Protocol (SNMP) feature that provides a method for managing network devices. It contains the following sections:

Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in the fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is composed of the enterprise number and the default MAC address. This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

Local information is stored in four MIB variables that are read only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).

⚠

Caution When the engine ID is changed, all configured users are erased.

To configure the SNMP engine ID, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Engine ID**.

Step 2 Choose which to use for Local Engine ID.

- Use Default—Select to use the device-generated engine ID. The default engine ID is based on the device MAC address.
- None—No engine ID is used.
- User Defined—Enter the local device engine ID. The field value is a hexadecimal string (range: 10–64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

  All remote engine IDs and their IP addresses are displayed in the Remote Engine ID table.

Step 3 Click **Apply**. The Running Configuration file is updated.

The Remote Engine ID table shows the mapping between the IP addresses of the engine and Engine ID.

To add the IP address of an engine ID:

Step 4 Click **Add**. Enter the following fields:

- Server Definition—Select whether to specify the Engine ID server by IP address or name.
- IP Version—Select the supported IP format.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
- Server IP Address/Name—Enter the IP address or domain name of the log server.
- Engine ID—Enter the Engine ID.

Step 5 Click **Apply**. The Running Configuration file is updated.

SNMP Views

A view is a user-defined label for a collection of MIB subtrees. Each subtree ID is defined by the Object ID (OID) of the root of the relevant subtrees. Either well-known names can be used to specify the root of the desired subtree or an OID can be entered. The Views page enables creating and editing SNMP views. The default views (Default, DefaultSuper) can't be changed.

Views can be attached to groups or to a community which employs basic access mode through the SNMP Groups, on page 3.

To configure the SNMP views, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Views**.

Step 2 Click **Add** to define new views.

Step 3 Enter the parameters.

- View Name—Enter a view name 0–30 characters.
- Object ID Subtree—Select the node in the MIB tree that is included or excluded in the selected SNMP view. The options to select the object are as follows:
  - Select from list—Enables you to navigate the MIB tree.
  - User Defined—Enter an OID not offered in the Select from list option.

Step 4 Select or deselect **Include in view.** If this is selected, the selected MIBs are included in the view, otherwise they are excluded.

Step 5 Click **Apply**.

Step 6 In order to verify your view configuration, select the user-defined views from the Filter: View Name list.

- Default—Default SNMP view for read and read/write views.
- DefaultSuper—Default SNMP view for administrator views.

SNMP Groups

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string is encrypted. Therefore, SNMPv1 and SNMPv2 aren't secure.

In SNMPv3, the following security mechanisms can be configured.

- Authentication—The device checks that the SNMP user is an authorized system administrator. This is done for each frame.
- Privacy—SNMP frames can carry encrypted data.

Thus, in SNMPv3, there are three levels of security:

- No security (No authentication and no privacy)
- Authentication (Authentication and no privacy)
- Authentication and privacy

SNMPv3 provides a means of controlling the content each user can read or write and the notifications they receive. A group defines read/write privileges and a level of security. It becomes operational when it's associated with an SNMP user or community.

Note To associate a non-default view with a group, first create the view in the SNMP Views, on page 2.

To create an SNMP group, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Groups**.

This page contains the existing SNMP groups and their security levels.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Group Name—Enter a new group name.
- Security Model—Select the SNMP version attached to the group, SNMPv1, v2, or v3.

  Three types of views with various security levels can be defined. For each security level, select the views for Read, Write, and Notify by entering the following fields:
- Enable—Select this field to enable the Security Level.
- Security Level—Define the security level attached to the group. SNMPv1 and SNMPv2 support neither authentication nor privacy. If SNMPv3 is selected, choose one of the following:
  - No Authentication and No Privacy—Neither the Authentication nor the Privacy security levels are assigned to the group.
  - Authentication and No Privacy—Authenticates SNMP messages, and ensures that the SNMP message origin is authenticated but doesn't encrypt them.
  - Authentication and Privacy—Authenticates SNMP messages, and encrypts them.
- View—Select to associate a view with either read, write, and/or notify access privileges of the group limits the scope of the MIB tree to which the group has read, write, and notify access.
  - Read—Management access is read-only for the selected view. Otherwise, a user or a community associated with this group is able to read all MIBs except those that control SNMP itself.
  - Write—Management access is written for the selected view. Otherwise, a user or a community associated with this group is able to write all MIBs except those that control SNMP itself.
  - Notify—Limits the available content of the traps to those included in the selected view. Otherwise, there's no restriction on the contents of the traps. This can only be selected for SNMPv3.

Step 4 Click **Apply**. The SNMP group is saved to the Running Configuration file.

SNMP Users

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID. The configured users have the attributes of its group, having the access privileges configured within the associated view.

To create an SNMPv3 user, the following must first exist:

- An engine ID must first be configured on the device. This is done in the Engine ID, on page 1.
- An SNMPv3 group must be available. An SNMPv3 group is defined in the SNMP Groups, on page 3.

To display SNMP users and define new ones:

Procedure

Step 1 Click **SNMP** > **Users**.

This page displays existing users. The fields in this page are described in the Add page except for the following field:

- IP Address—Displays the IP address of the engine.

Step 2 Click **Add.**

This page provides information for assigning SNMP access control privileges to SNMP users.

Step 3 Enter the parameters.

- User Name—Enter a name for the user.
- Engine ID—Select either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database. To receive inform messages and request information, you must define both a local and remote user.
  - Local—User is connected to the local device.
  - Remote IP Address—User is connected to a different SNMP entity in addition to the local device. If the remote Engine ID is defined, remote devices receive inform messages, but can't make requests for information.
- Group Name—Select the SNMP group to which the SNMP user belongs. SNMP groups are defined in the Add Group page.

  Note
  Users who belong to groups which have been deleted, remain, but they are inactive.

- Authentication Method—Select the desired Authentication method that varies according to the Group Name assigned. If the group doesn't require authentication, then the user can't configure any authentication. The options are:
  - None—No user authentication is used.
  - SHA—A password that is used for generating a key by the SHA-1 (Secure Hash Algorithm) authentication method.

- SHA224— A password that is used for generating a key by the SHA-224 (based on Secure Hash Algorithm 2) authentication method truncated to 128 bits.
- SHA256—A password that is used for generating a key by the SHA-256 (based on Secure Hash Algorithm 2) authentication method truncated to 192 bits.
- SHA384— A password that is used for generating a key by the SHA-384 (based on Secure Hash Algorithm 2) authentication method truncated to 256 bits.
- SHA512—A password that is used for generating a key by the SHA-512 (based on Secure Hash Algorithm 2) authentication method truncated to 384 bits.

- Authentication Password—If authentication is accomplished by password and authentication method, enter the local user password in either Encrypted or Plaintext. Local user passwords are compared to the local database and can contain up to 64 ASCII characters.
- Privacy Method—Select one of the following options:
  - None—Privacy password isn't encrypted.
  - AES—Privacy password is encrypted according to the AES.
- Privacy Password—If you choose the AES privacy method, you need 16 bytes (the AES encryption key). This field must have precisely 64 hexadecimal characters. You have the option of using Encrypted or Plaintext mode.

Step 4 Click **Apply** to save the settings.

SNMP Communities

Access rights in SNMPv1 and SNMPv2 are managed by defining communities in the Communities page. The community name is a type of shared password between the SNMP management station and the device. It's used to authenticate the SNMP management station.

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them. The Communities page associates communities with access rights, either directly (Basic mode) or through groups (Advanced mode):

- Basic Mode—The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view (defined in the SNMP Users, on page 5).
- Advanced Mode—The access rights of a community are defined by a group (defined in the SNMP Groups, on page 3). You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

To define the SNMP communities, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Communities**.

Step 2 Click **Add** to define and configure new SNMP community.

Step 3 Configure the following fields:

SNMP Management Station	Select one of the following options: • All—to indicate that any IP device can access the SNMP community. • User Defined—to enter the management station IP address that can access the SNMP community.
IP Version	Select either IPv4 or IPv6.
IPv6 Address Type	Select the supported IPv6 address type if IPv6 is used. The options are: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If the IPv6 address type is Link Local, select whether it's received through a VLAN or ISATAP.
IP Address	Enter the SNMP management station IP address.
Community String	Enter the community name used to authenticate the management station to the device.
Basic	In this community type, there's no connection to any group. You can only choose the community access level (Read Only, Read Write, or SNMP Admin) and, optionally, further qualify it for a specific view. By default, it applies to the entire MIB. If this is selected, enter the following fields: • Access Mode—Select the access rights of the community. The options are: Read Only—Management access is restricted to read-only. Changes can't be made to the community. Read Write—Management access is read-write. Changes can be made to the device configuration, but not to the community. SNMP Admin—User has access to all device configuration options, and permissions to modify the community. SNMP Admin is equivalent to Read Write for all MIBs except for the SNMP MIBs. SNMP Admin is required for access to the SNMP MIBs. • View Name—Select an SNMP view (a collection of MIB subtrees to which access is granted).
Advanced	Select this type for a selected community. • Group Name—Select an SNMP group that determines the access rights.

Step 4 Click **Apply**. The SNMP Community is defined, and the Running Configuration is updated.

Trap Settings

The Trap Settings page enables configuring whether SNMP notifications are sent from the device, and for which cases.

To define trap settings, follow these steps:

Procedure

Step 1 Click **SNMP** > **Trap Settings**.

Step 2 Select **Enable** for SNMP Notifications to specify that the device can send SNMP notifications.

Step 3 Select **Enable** for Authentication Notifications to enable SNMP authentication failure notification.

Step 4 Click **Apply**. The SNMP Trap settings are written to the Running Configuration file.

Notification Recipients SNMPv1,2

The notification recipients enable configuring the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). An SNMP notification is a message sent from the device to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

It is also possible to filter certain notifications. This can be done by creating a filter in the Notification Filter, on page 11 and attaching it to an SNMP notification recipient. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification that is about to be sent.

To define a recipient in SNMPv1,2:

Procedure

Step 1 Click **SNMP** > **Notification Recipients SNMPv1,2**.

This page displays recipients for SNMPv1,2.

Step 2 Enter the following fields:

- Informs IPv4 Source Interface—Select an option (Auto or VLAN1) from the drop-down that will be used as the source IPv4 address in trap messages for communication with IPv4 SNMP servers.
- Traps IPv4 Source Interface—Select an option (Auto or VLAN1) from the drop-down that will be used as the source IPv4 address in trap messages for communication with IPv4 SNMP servers.

- Informs IPv6 Source Interface—Select an option (Auto or VLAN1) from the drop-down that will be used as the source IPv6 address in inform messages for communication with IPv6 SNMP servers.
- Traps IPv6 Source Interface—Select an option (Auto or VLAN1) from the drop-down that will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.

Note
If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Add.**

Step 4 Enter the parameters.

- Server Definition—Select whether to specify the remote log server by IP address or name.
- IP Version—Select either IPv4 or IPv6.
- IPv6 Address Type—Select either Link Local or Global.
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—If the IPv6 address type is Link Local, select whether it's received through a VLAN or ISATAP.
- Recipient IP Address/Name—Enter the IP address or server name of where the traps are sent.
- UDP Port—Enter the UDP port used for notifications on the recipient device.
- Notification Type—Select whether to send Traps or Informs. If both are required, two recipients must be created.
- Timeout—Enter the number of seconds the device waits before resending informs.
- Retries—Enter the number of times that the device resends an inform request.
- Community String—Select from the pull-down the community string of the trap manager. Community String names are generated from those listed in the SNMP Communities, on page 6.
- Notification Version—Select the trap SNMP version. Either SNMPv1 or SNMPv2 may be used as the version of traps, with only a single version enabled at a time.
- Notification Filter—Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the Notification Filter, on page 11.
- Filter Name—Select the SNMP filter that defines the information contained in traps (defined in the Notification Filter, on page 11).

Step 5 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Notification Recipients SNMPv3

To define a recipient in SNMPv3:

Procedure

Step 1 Click **SNMP** > **Notification Recipients SNMPv3**.

Step 2 Configure the following settings:

- Informs IPv4 Source Interface—From the drop-down list, select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv4 Source Interface—From the drop-down list, select the source interface whose IPv4 address will be used as the source address in trap messages.
- Informs IPv6 Source Interface—From the drop-down list, select the source interface whose IPv6 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv6 Source Interface—From the drop-down list, select the source interface whose IPv6 address will be used as the source address in trap messages.

Step 3 Click **Add.**

Step 4 Enter the parameters.

- Server Definition—Select whether to specify the remote log server by IP address or name.
- IP Version—Select either IPv4 or IPv6.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the pull-down list.
- Recipient IP Address/Name—Enter the IP address or server name of where the traps are sent.
- UDP Port—Enter the UDP port used to for notifications on the recipient device.
- Notification Type—Select whether to send traps or informs. If both are required, two recipients must be created.
- Timeout—Enter the amount of time (seconds) the device waits before resending informs/traps. Time out: Range 1-300, default 15
- Retries—Enter the number of times that the device resends an inform request. Retries: Range 0-255, default 3
- User Name—Select from the drop-down list the user to whom SNMP notifications are sent. To receive notifications, this user must be defined on the page , and its engine ID must be remote.

- Security Level—Select how much authentication is applied to the packet.

  Note
  The Security Level here depends on which User Name was selected. If this User Name was configured as No Authentication, the Security Level is No Authentication only. However, if this User Name has been assigned with Authentication and Privacy rights, the security level can be either No Authentication, or Authentication Only, or Authentication and Privacy.

  The options are:

  - No Authentication—Indicates that the packet isn't authenticated or encrypted.
  - Authentication—Indicates that the packet is authenticated but not encrypted.
  - Privacy—Indicates that the packet is both authenticated and encrypted.

- Notification Filter—Select to enable filtering the type of SNMP notifications sent to the management station.
- Filter Name—Select the SNMP filter that defines the information contained in traps.

Step 5 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Notification Filter

The Notification Filter page enables configuring SNMP notification filters and Object IDs (OIDs) that are checked. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification to be sent.

To define a notification filter:

Procedure

Step 1 Click **SNMP** > **Notification Filter**.

The Notification Filter Table contains notification information for each filter. The table is able to filter notification entries by Filter Name. The Object Identifier Tree Filter displays the current status of each configured filter.

Step 2 Click **Add** to add a Notification Filter or click **Edit** to edit an existing Notification Filter.

Step 3 Enter or modify the following parameters:

- Filter Name—Enter a name between 0-30 characters.
- Object ID Subtree—Select the node in the MIB tree that is included or excluded in the selected SNMP filter. The options to select the object are as follows:
  - Select from List—Enables you to navigate the MIB tree. Press the Up arrow to go to the level of the selected node's parent and siblings; press the Down arrow to descend to the level of the selected node's children. Click nodes in the view to pass from one node to its sibling. Use the scrollbar to bring siblings in view.
  - Object ID—Select this option to include the entered object identifier in the view, if the Include in filter option is selected.

Step 4 Select or deselect **Include in filter.** If this is selected, the selected MIBs are included in the filter, otherwise they are excluded.

Step 5 Click **Apply**. The SNMP views are defined and the running configuration is updated.