

Configure Simple Network Management Protocol (SNMP) Users on a Switch

Objective

Simple Network Management Protocol (SNMP) is a network management protocol which helps to record, store, and share information about the devices in the network. This helps the administrator address network issues. SNMP uses Management Information Bases (MIBs) to store available information in a hierarchical manner. An SNMP User is defined by login credentials such as username, password, and authentication method. It is operated in association with an SNMP group and an engine ID. For instructions on how to configure an SNMP Group, click [here](#). Only SNMPv3 use SNMP users. Users with access privileges are associated with an SNMP view.

For example, SNMP users might be configured by a network manager to associate them to a group so that access rights can be assigned to a group of users in that particular group rather than to a single user. A user can only belong to one group. In order to create an SNMPv3 User, an Engine ID must be configured and an SNMPv3 Group must be available.

This document explains how to create and configure an SNMP user on a switch.

Applicable Devices

- Sx250 Series
- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Software Version

- 1.4.7.05 — Sx300, Sx500
- 2.2.8.04 — Sx250, Sx350, SG350X, Sx550X

Configure SNMP Users on a Switch

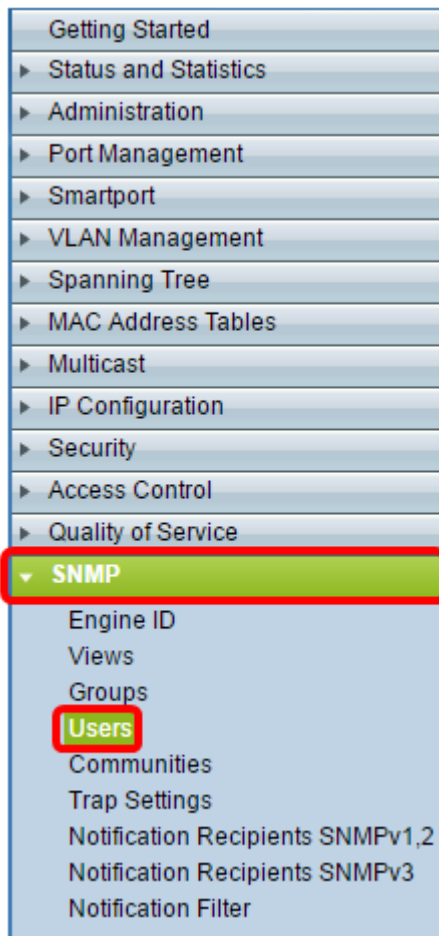
Add an SNMP User

Step 1. Log in to the web-based utility of the switch.

Step 2. Change the Display Mode to **Advanced**.

Note: This option is not available on the SG300 Series and SG500 Series switch. If you have those models, skip to [Step 3](#).

Step 3. Choose **SNMP > Users**.



Step 4. Click **Add** to create a new SNMP user.



Step 5. Enter the name of the SNMP user in the *User Name* field.



The image shows a configuration dialog box for SNMP. It contains the following fields and options:

- User Name:** A text box containing "SNMP_User1" with a red border. To its right, it says "(10/20 characters used)".
- Engine ID:** Two radio button options: "Local" (selected) and "Remote IP Address" (with a dropdown arrow).
- Group Name:** A dropdown menu showing "SNMP_Group".
- Authentication Method:** Three radio button options: "None", "MD5", and "SHA" (selected).
- Authentication Password:** Two radio button options: "Encrypted" (disabled) and "Plaintext" (selected). The "Plaintext" option has a text box containing "password1" and "(9/32 characters used)". Below it, a note says "(The password is used for generating a key)".
- Privacy Method:** Two radio button options: "None" and "DES" (selected).
- Privacy Password:** Two radio button options: "Encrypted" (disabled) and "Plaintext" (selected). The "Plaintext" option has a text box containing "password2" and "(9/32 characters used)". Below it, a note says "(The password is used for generating a key)".

At the bottom of the dialog, there are two buttons: "Apply" and "Close".

Note: In this example, the user name is SNMP_User1.

Step 6. Click the Engine ID. The options are:

- Local – This option means that the user is connected to the local switch.
- Remote IP Address – This option means that the user is connected to a different SNMP entity besides the local switch. Choose a remote IP address from the IP address drop-down list. This remote IP address is the IP address configured for the SNMP engine ID.

* User Name: (10/20 characters used)

* Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: None
 MD5
 SHA

* Authentication Password: Encrypted
 Plaintext (9/32 characters used)
 (The password is used for generating a key)

Privacy Method: None
 DES

* Privacy Password: Encrypted
 Plaintext (9/32 characters used)
 (The password is used for generating a key)

Note: When the local SNMP Engine ID is changed or removed, it deletes the SNMPv3 User database. In order for the inform messages and request information to be received, both the local and the remote user must be defined. In this example, Local is chosen.

Step 7. Choose the SNMP group name where the SNMP user belongs from the Group Name drop-down list.

* User Name: (10/20 characters used)

* Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: SNMP_Group
 MD5
 SHA

* Authentication Password: Encrypted
 Plaintext (9/32 characters used)
 (The password is used for generating a key)

Privacy Method: None
 DES

* Privacy Password: Encrypted
 Plaintext (9/32 characters used)
 (The password is used for generating a key)

Note: In this example, SNMP_Group is chosen.

Step 8. Click the authentication method. The options are:

- None — This option means that there is no user authentication used.
- MD5 — This option means that the password entered by the user is encrypted with MD5. MD5 is a cryptographic function which has a 128-bit hash value. It is commonly used for data entry.
- SHA — This option means that the password entered by the user is encrypted with Secure Hash Algorithm (SHA) authentication method. Hash functions are used to convert an input of arbitrary size to an output of fixed size which would be a 160-bit hash value.

The screenshot shows a configuration window with the following fields and options:

- User Name:** SNMP_User1 (10/20 characters used)
- Engine ID:** Local, Remote IP Address
- Group Name:** SNMP_Group
- Authentication Method:** None, MD5, SHA
- Authentication Password:** Encrypted, Plaintext (password1) (9/32 characters used)
(The password is used for generating a key)
- Privacy Method:** None, DES
- Privacy Password:** Encrypted, Plaintext (password2) (9/32 characters used)
(The password is used for generating a key)

Buttons: Apply, Close

Note: In this example, SHA is chosen.

Step 9. Click the radio button for the Authentication Password. The options are:

- Encrypted — This option means that the password will be encrypted. It will not be shown as it is entered.
- Plaintext — This option means that the password will not be encrypted. It will be shown as it is being entered.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Note: In this example, Plaintext is chosen.

Step 10. Enter the password.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Note: In this example, the password is password1.

Step 11. Click a Privacy Method. The options are:

- None — This option means that the password is not encrypted.
- DES — This option means that the password is encrypted with Data Encryption Standard (DES). DES is a standard which takes a 64-bit input value and uses a 56-bit key for encryption and decryption of the messages. It is a symmetric encryption algorithm where the sender and the receiver use the same key.

The screenshot shows a configuration window with the following fields and options:

- User Name:** SNMP_User1 (10/20 characters used)
- Engine ID:** Local (selected), Remote IP Address (dropdown)
- Group Name:** SNMP_Group (dropdown)
- Authentication Method:** None, MD5, SHA (SHA is selected)
- Authentication Password:** Encrypted (disabled), Plaintext (selected, password1) (9/32 characters used). Note: (The password is used for generating a key)
- Privacy Method:** None, DES (selected and circled in red)
- Privacy Password:** Encrypted (disabled), Plaintext (selected, password2) (9/32 characters used). Note: (The password is used for generating a key)

Buttons: Apply, Close

Note: Privacy Methods can be configured only for groups with Authentication and Privacy configured. For more information, click [here](#). In this example, DES is chosen.

Step 12. (Optional) If DES is chosen, choose the Privacy Password authentication. The options are:

- Encrypted — This option means that the password will be encrypted. It will not be shown as it is entered.
- Plaintext — This option means that the password will not be encrypted. It will be shown as it is being entered.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Note: In this example, Plaintext is chosen.

Step 13. Enter the DES Password.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:

Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Note: In this example, the DES password is password2.

Step 14. Click **Apply** then click **Close**.

User Name: (10/20 characters used)

Engine ID: Local Remote IP Address

Group Name:

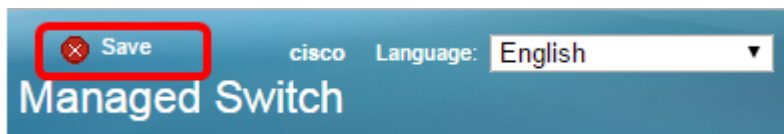
Authentication Method: None MD5 SHA

Authentication Password: Encrypted Plaintext (9/32 characters used)
 (The password is used for generating a key)

Privacy Method: None DES

Privacy Password: Encrypted Plaintext (9/32 characters used)
 (The password is used for generating a key)

Step 15. (Optional) Click **Save**.



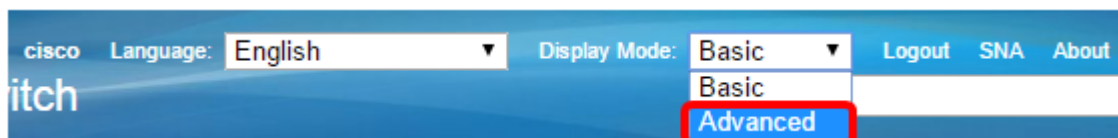
You should now have added an SNMP User to your switch.

Modify SNMP Users

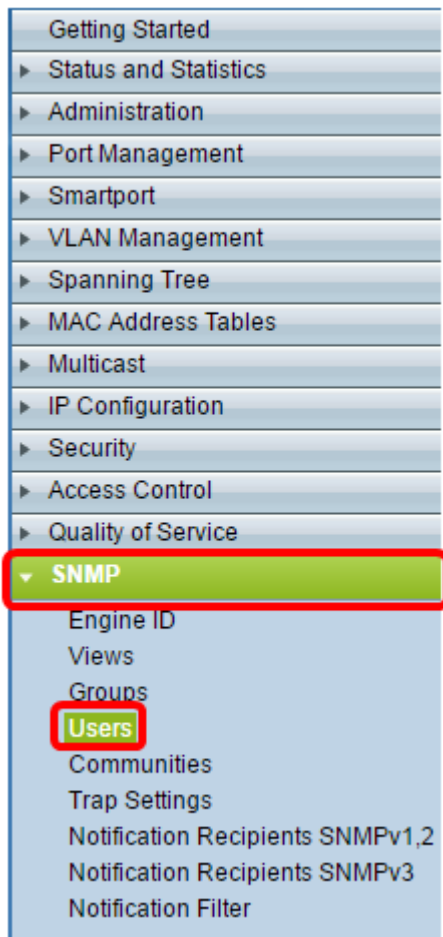
Step 1. Log in to the web-based utility of the switch.

Step 2. Change the Display Mode to **Advanced**.

Note: This option is not available on the SG300 Series and SG500 Series switch. If you have those models, skip to [Step 3](#).



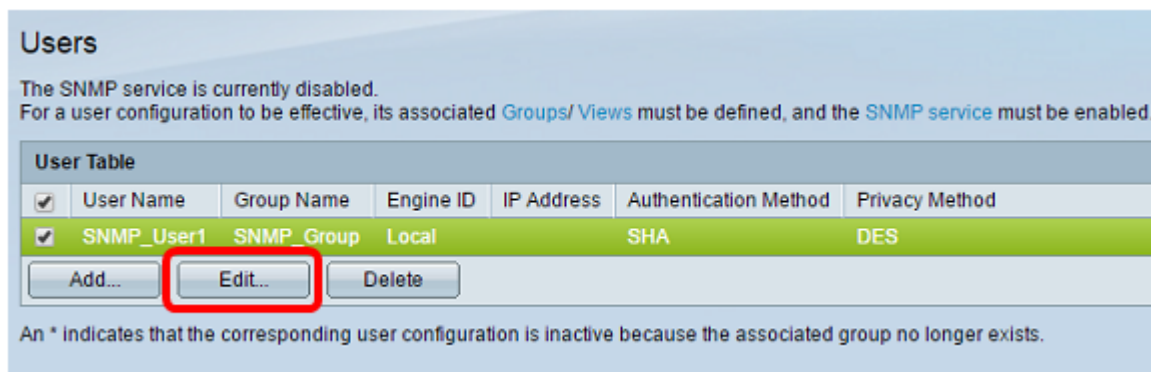
[Step 3](#). Choose **SNMP > Users**.



Step 4. Check the check box that corresponds to the User that you want to edit.



Step 5. Click **Edit**.



Step 6. Edit the settings that need to be changed.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:
Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Step 7. Click **Apply** then click **Close**.

User Name: (10/20 characters used)

Engine ID: Local
 Remote IP Address

Group Name:
Authentication Method: None
 MD5
 SHA

Authentication Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Privacy Method: None
 DES

Privacy Password: Encrypted
 Plaintext (9/32 characters used)
(The password is used for generating a key)

Step 8. (Optional) Click **Save**.

cisco Language:

Managed Switch

You should now have successfully edited the SNMP User settings.