

Simple Network Management Protocol (SNMP) User Configuration on 300 Series Managed Switches

Objective

SNMP is a network management protocol which is used for managing network devices. It helps to record, store and share the information of various devices in the network that facilitates the administrator to solve the network issues quickly. SNMP uses Management Information Bases (MIBs) to store available information in a hierarchical manner. You can configure SNMP users. These users will be part of a SNMP group, which gives the users the SNMP attributes and access privileges. This article explains how to create SNMP users on the 300 Series Managed Switches.

Note: SNMP must be enabled on the switch to work properly. For more information on how to enable SNMP refer to the article *Enable Simple Network Management Protocol (SNMP) Service on 300 Series Managed Switches*.

Applicable Devices

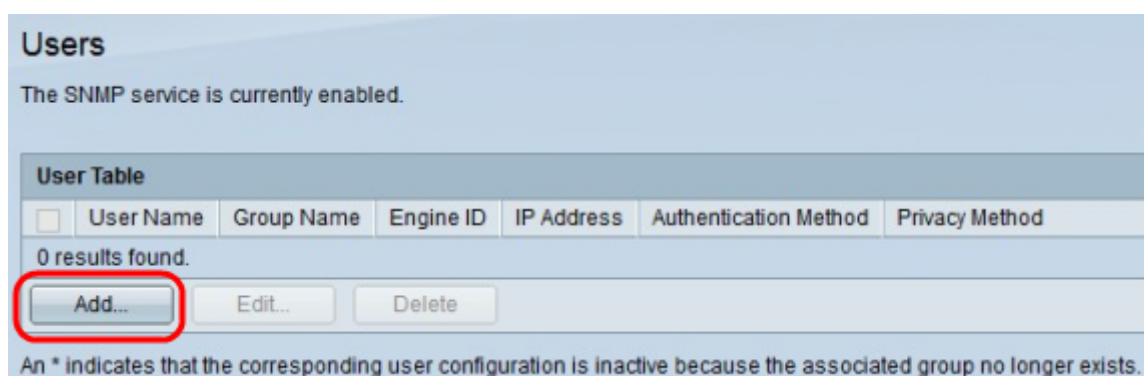
- SF/SG 300 Series Managed Switches

Software Version

- 1.3.0.62

SNMP User Configuration

Step 1. Log in to the web configuration utility and choose **SNMP > Users**. The *Users* page opens:



Step 2. Click **Add**. The *Add User* window appears.

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

- User Name:** A text field containing "username1" with a character count of "(9/20 Characters Used)".
- Engine ID:** Two radio buttons: "Local" (selected) and "Remote IP Address" (with a dropdown arrow).
- Group Name:** A dropdown menu showing "Group1".
- Authentication Method:** Three radio buttons: "None", "MD5", and "SHA" (selected).
- Authentication Password:** Two radio buttons: "Encrypted" (with a greyed-out field) and "Plaintext" (selected). The plaintext field contains "password1" with a character count of "(9/32 Characters Used)". A note below states: "(The password is used for generating a key)".
- Privacy Method:** Two radio buttons: "None" and "DES" (selected).
- Privacy Password:** Two radio buttons: "Encrypted" (with a greyed-out field) and "Plaintext" (selected). The plaintext field contains "password2" with a character count of "(9/64 Characters Used)". A note below states: "(The password is used for generating a key)".

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

Step 3. Enter a username for the user in the User Name field.

Step 4. Click the specific radio button to choose the appropriate Engine ID. The engine ID is the device that provides SNMP capabilities to the user. The available options are:

- Local — This option chooses the local switch as the engine ID.
- Remote IP Address — This option chooses the IP of an already configured engine ID which provides SNMP capabilities to the users of the switch.

Note: For more information on how to configure an engine ID, refer to the article *Configure Simple Network Management Protocol (SNMP) Engine ID on 300 Series Managed Switches*.

Step 5. Choose from the Group Name drop-down list, the SNMP group to which you wish this user to be part of.

Note: For more information on how to create a SNMP group, refer to the article *Simple Network Management Protocol (SNMP) Group Configuration on a 300 Series Managed Switch*.

Step 6. Click the radio button of an authentication method. The available options are:

- None — No user authentication is used.
- MD5 Password — The password which is provided by the user is encrypted using the MD5 authentication method. MD5 is a cryptographic hash function which has a 128-bit hash value and is commonly used for data integrity.
- SHA Password — The password which is provided by the user is encrypted using the 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.

Step 7. Click the radio button of an authentication password option in the Authentication Password field. The available options are:

- Encrypted — This option lets you enter an already encrypted password.
- Plaintext — This option lets you enter a password as a plain text.

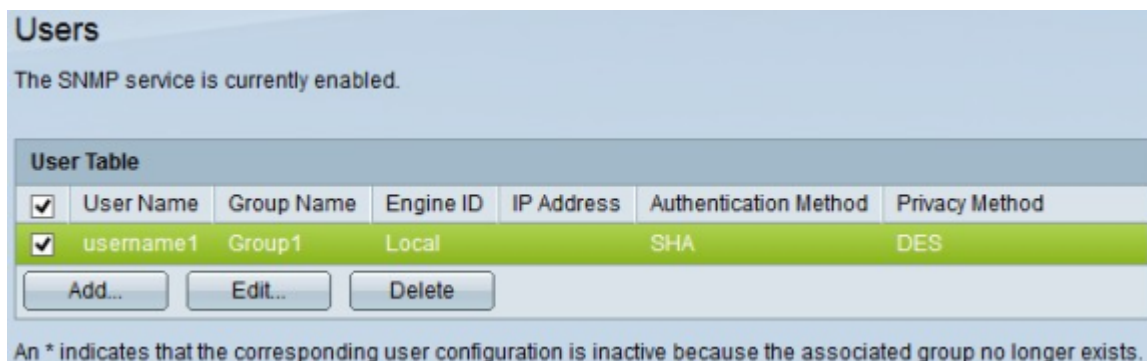
Step 8. Click the radio button of a privacy method in the Privacy Method field. The available options are:

- None —The privacy password is not encrypted.
- DES —The privacy password is encrypted with the 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.

Step 9. Click the radio button to enter a privacy password in the Privacy Password field. The available options are:

- Encrypted —This option lets you enter an encrypted privacy password
- Plaintext —This option lets you enter a privacy password as a plain text.

Step 10. Click **Apply** to save your configuration.



The screenshot shows a web interface for managing users. At the top, it says "Users" and "The SNMP service is currently enabled." Below this is a "User Table" with the following columns: User Name, Group Name, Engine ID, IP Address, Authentication Method, and Privacy Method. There is one row with the following values: username1, Group1, Local, (blank), SHA, and DES. There are checkboxes in the first column, with the one for 'username1' checked. Below the table are three buttons: "Add...", "Edit...", and "Delete...". At the bottom, a note states: "An * indicates that the corresponding user configuration is inactive because the associated group no longer exists."

| <input type="checkbox"/> | User Name | Group Name | Engine ID | IP Address | Authentication Method | Privacy Method |
|-------------------------------------|-----------|------------|-----------|------------|-----------------------|----------------|
| <input checked="" type="checkbox"/> | username1 | Group1 | Local | | SHA | DES |

Step 11. (Optional) To edit a user, check the check box of the user you wish to edit and click **Edit**.

Step 12. (Optional) To delete a user, check the check box of the user you wish to delete and click **Delete**.