

Configure SNMP Groups on a Switch through the CLI

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. SNMP Groups are used to combine the SNMP users based on access privileges and authorization to different SNMP views at the MIBs. Each SNMP group is uniquely identified by a combination of group name and the security levels.

This document explains how to create and configure an SNMP group using the Command Line Interface of a switch. It assumes that SNMP Views has already been configured for the device.

SNMP groups can also be configured through the web-based utility of the switch. For instructions, refer to [Configure Simple Network Management Protocol \(SNMP\) Groups on a Switch](#).

Applicable Devices

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

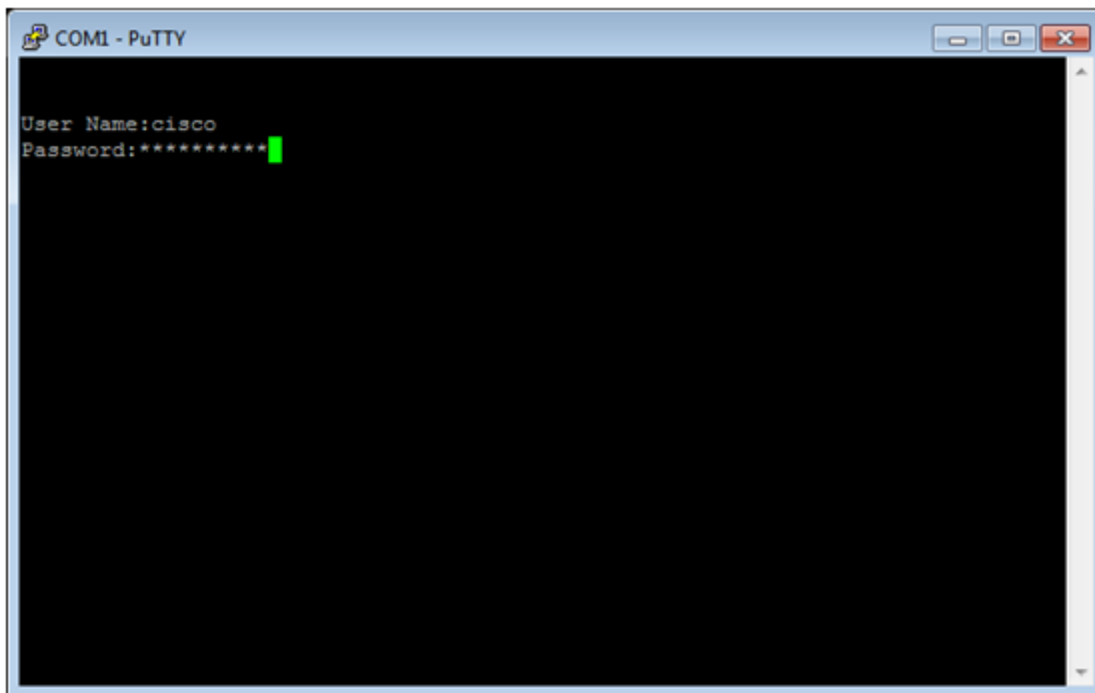
Software Version

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

Configure SNMP Groups on a Switch

Step 1

Access the CLI of the switch.



In this example, PuTTY is the application used to access the switch CLI. The default username and password is cisco/cisco. If you have customized your credentials, use your username and password.

Step 2

Switch to Global Configuration mode by entering the following command:

```
Switch350X#configure terminal
```

Step 3

Create an SNMP Group using the following syntax:

```
snmp-server group groupname{v1/v2/v3 {{noauth/auth/priv}}[notify notifyview]]}[read readview]  
[write writeview].
```

Where:

- group *groupname* - This is where you can specify the name of the group. The *groupname* can be 1 to 30 characters in length.
- v1 - This option uses the SNMP version 1 security model.
- v2 - This option uses the SNMP version 2 security model
- v3 - This option uses the SNMP version 3 security model.
- noauth - This option specifies that no packet authentication will be performed. This option is applicable only to the SNMPv3 security model.
- auth - This option specifies that packet authentication without encryption will be performed. This option is applicable only to the SNMPv3 security model.
- priv - This option specifies that packet authentication with encryption will be performed. This option is applicable only to the SNMPv3 security model.
- notify *notifyview* - (Optional) This option specifies the view name that enables generating informs or a trap. An inform is a trap that requires acknowledgement. This option is available only on the SNMPv3 security model.

- read readview - (Optional) This option specifies the view name that enables viewing only. The view name can be between 1 to 30 characters in length.
- write writeview - (Optional) This option specifies the view name that enables configuring the agent. The view name can be 1 to 30 characters.

```
Switch350X#snmp-server group CiscoTestUsers v3 auth notify Cisco1234$ read
```

In this example, snmp-server group CiscoTestUsers v3 auth notify Cisco1234\$ read is entered.

Step 4

Verify SNMP group using the following command:

```
Switch350X#show snmp groups
```

You should now have configured an SNMP Group settings through the CLI of the switch.