

# Configure Simple Network Management Protocol (SNMP) Notification Recipients on a Switch

## Objective

Simple Network Management Protocol (SNMP) is a network management protocol which helps record, store, and share information about the devices in the network. This helps the administrator address network issues. SNMP notification messages, or traps, report system events such as the temperature of a remote device. Traps are sent from an SNMP-enabled network device to network management stations that help troubleshoot network issues easily. The system can generate traps in the Management Information Base (MIB) that it supports.

The following configurations are prerequisites of being able to configure SNMP notification recipients successfully:

- SNMP Communities — This is required for SNMPv1 and SNMPv2. For instructions on configuring SNMP Communities, click [here](#).
- SNMP Users — This is required for SNMPv3. For instructions on configuring SNMP Users, click [here](#).

This document aims to show you how to configure the destination (notification recipient) to which SNMP notifications (traps or informs) are sent, and the types of SNMP notifications that are sent to each destination 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

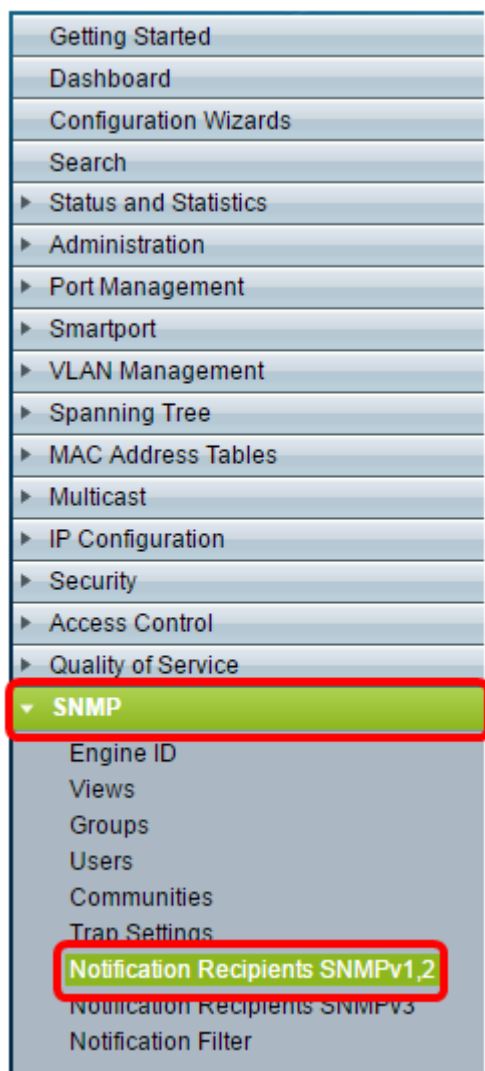
## Configure SNMP Notification Recipients

### Configure SNMPv1,2 Notification Recipients

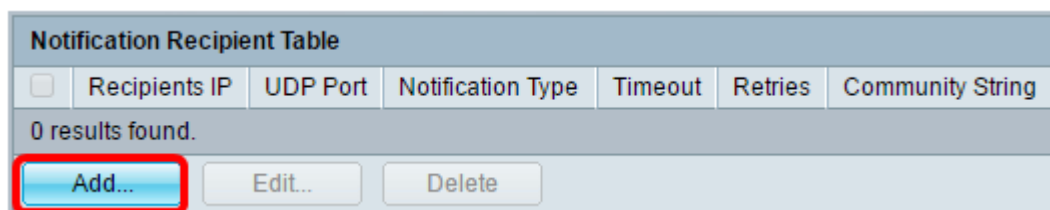
Step 1. Log in to the web-based utility of the switch.

Step 2. Choose **Advanced** from the Display Mode drop-down list.

Step 3. Choose **SNMP > Notification Recipients SNMPv1,2**.



Step 4. Click **Add**.



Step 5. Choose an Internet Protocol (IP) version. The options are:

- Version 6 — Choose this option if the Management station has an IPv6 address type.
- Version 4 — Choose this option if the Management station has an IPv4 address type.

Server Definition:  By IP address  By name  
IP Version:  Version 6  Version 4  
IPv6 Address Type:  Link Local  Global  
Link Local Interface:

**Note:** In this example, Version 6 is chosen.

Step 6. (Optional) If Version 6 is chosen, choose an IPv6 address type. The options are:

- Link Local — This IPv6 address has a prefix of FE80, which identifies hosts on a single network link. Link Local address types can only be used for communication on the local network.
- Global — This IPv6 address type is visible to other networks.

Server Definition:  By IP address  By name  
IP Version:  Version 6  Version 4  
IPv6 Address Type:  Link Local  Global  
Link Local Interface:

**Note:** In this example, Link Local is chosen.

Step 7. (Optional) If the IPv6 address type is Link Local, choose the interface through which address is received from the Link Local Interface drop-down list.

Server Definition:  By IP address  By name  
IP Version:  Version 6  Version 4  
IPv6 Address Type:  Link Local  Global  
Link Local Interface:   
Recipient IP Address/Name:   
UDP Port:  (Range: 1 - 65535, Default: 162)

**Note:** In this example, Link Local Interface is VLAN 1.

Step 8. Enter the IP address of the recipient device in the *Recipient IP Address/Name* field.

Server Definition:  By IP address  By name  
IP Version:  Version 6  Version 4  
IPv6 Address Type:  Link Local  Global  
Link Local Interface:   
Recipient IP Address/Name:   
UDP Port:  (Range: 1 - 65535, Default: 162)

**Note:** In this example, the Recipient IP Address/Name is fe80:0::eebd:1dff:fe44:5719.

Step 9. Enter the User Datagram Protocol (UDP) port used for notification on the recipient

device in the *UDP Port* field.

Server Definition:  By IP address  By name  
IP Version:  Version 6  Version 4  
IPv6 Address Type:  Link Local  Global  
Link Local Interface:   
Recipient IP Address/Name:   
UDP Port:  (Range: 1 - 65535, Default: 162)

**Note:** In this example, 162 is entered.

**Step 10.** Choose a Notification Type. The options are:

- Traps — This option reports system events. This type of notification is unacknowledged.
- Informs — This option is similar to a Trap. The main difference is that an Inform is an acknowledged form of Trap. This type of notification is available in SNMPv2.

**Note:** If Informs is chosen, proceed to [Step 11](#). If Traps is chosen, proceed to [Step 13](#).

Notification Type:  Traps  Informs  
Timeout:  sec (Range: 1 - 300, Default: 15)  
Retries:  (Range: 1 - 255, Default: 3)

**Note:** In this example, Informs is chosen.

**Step 11.** (Optional) Enter the number of seconds the device waits before resending Informs in the *Timeout* field. Valid values are from 1 to 300. The default value is 15.

Notification Type:  Traps  Informs  
Timeout:  sec (Range: 1 - 300, Default: 15)  
Retries:  (Range: 1 - 255, Default: 3)

**Note:** In this example, 22 is entered.

**Step 12.** (Optional) Enter the number of times that the device would attempt to send an Inform request in the *Retries* field. Valid values are from 1 to 255. The default value is 3 times.

Notification Type:  Traps  Informs  
Timeout:  sec (Range: 1 - 300, Default: 15)  
Retries:  (Range: 1 - 255, Default: 3)

**Note:** In this example, 5 is entered.

[Step 13.](#) Choose the community for the notification recipient from the Community String drop-down list.

Community String:

Notification Version:  SNMPv1  
 SNMPv2

**Note:** In this example, TestCommunity is chosen.

Step 14. Choose a Notification Version. The options are:

- SNMPv1 — This option utilizes SNMPv1.
- SNMPv2 — This option utilizes SNMPv2.

Community String:

Notification Version:  SNMPv1  
 SNMPv2

**Note:** In this example, SNMPv1 is chosen.

[Step 15.](#) (Optional) Check the Notification Filter **Enable** check box to filter the type of SNMP notifications sent to the management station.

Notification Filter:  Enable

Filter Name:

**Note:** In this example, the Notification Filter check box is checked.

[Step 16.](#) (Optional) If Notification Filter is enabled, choose the SNMP filter that defines the information contained in Traps from the Filter Name drop-down list.

Notification Filter:  Enable

Filter Name:

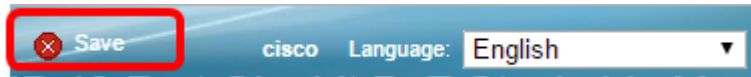
**Note:** In this example, TestFilter is chosen.

Step 17. Click **Apply** to save the configuration.

Notification Filter:  Enable

Filter Name:

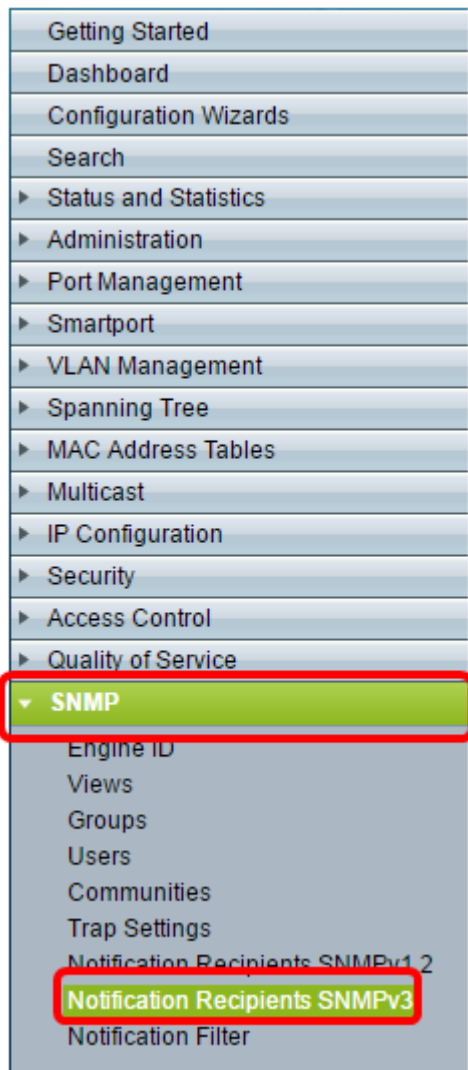
Step 18. Click **Save** to save to startup config file.



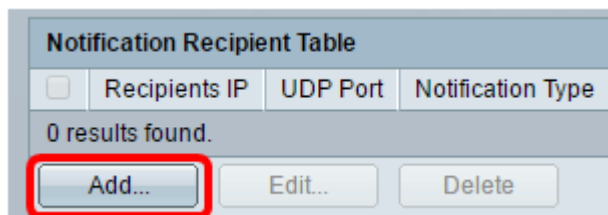
You should now have successfully added SNMP notifications on your switch.

## Configure SNMPv3 Notification Recipients

Step 1. Log in to the web-based utility and choose **SNMP > Notification Recipients SNMPv3**.



Step 2. Click **Add** to add a new notification recipient.



Step 3. Follow [Step 5](#) to [Step 10](#) of the Configuration of SNMPv1,2 Notification Recipients section of this article.

Step 4. Choose the User for the SNMPv3 notification recipient from the User Name drop-

down list.

User Name:

Security Level:  Authentication  Privacy

**Note:** In this example, SNMP Manager1 is chosen.

Step 5. Choose a Security Level. The options are:

- No Authentication — This indicates that the packet is neither authenticated nor encrypted.
- Authentication — This option indicates that the packet is authenticated but not encrypted.
- Privacy — This option indicates that the packet is both authenticated and encrypted.

User Name:

Security Level:  No Authentication  Authentication  Privacy

**Note:** The security level depends on the chosen User Name. If no authentication is configured for a User, the available Security Level would be No Authentication only.

Step 6. Follow [Step 15](#) to [Step 16](#) of the Configuration of SNMPv1,2 Notification Recipients section of this article.

Step 7. Click **Apply** to save the configuration.

Notification Filter:  Enable

Filter Name:

Step 8. Click **Save**.

cisco Language:

You should now have successfully added SNMPv3 Notification recipients on your switch.