



Configuring SNMP

This chapter contains the following sections:

- [Information About SNMP, page 1](#)
- [Guidelines and Limitations for SNMP, page 5](#)
- [Default Settings for SNMP, page 5](#)
- [Configuring SNMP, page 5](#)
- [Verifying the SNMP Configuration, page 14](#)
- [MIBs, page 15](#)
- [Feature History for SNMP, page 16](#)

Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

SNMP is defined in RFCs 3411 to 3418.

**Note**

SNMP Role Based Access Control (RBAC) is not supported.

Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

Cisco NX-OS generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The Cisco NX-OS cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the Cisco NX-OS never receives a response, it can send the inform request again.

You can configure Cisco Nexus NX-OS to send notifications to multiple host receivers.

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with while it was in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

The following table identifies what the combinations of security models and levels mean.

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

Cisco NX-OS uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

The Cisco NX-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The priv option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The priv option with the aes-128 token indicates that this privacy password is for generating a 128-bit AES key. The

AES priv password can have a minimum of eight characters. If the passphrases are specified in cleartext, you can specify a maximum of 64 case-sensitive, alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.



Note For an SNMPv3 operation that uses the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco NX-OS to leverage the user authentication service of the AAA server. After user authentication is verified, the SNMP PDUs are processed. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco NX-OS synchronizes a user configuration in the following ways:

- The authentication passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes the authentication and privacy passphrases for the SNMP user.
- If you delete a user using either SNMP or the CLI, the user is deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.



Note When you configure passphrase/password in localized key/encrypted format, Cisco NX-OS does not synchronize the user information (password, roles, and so on).

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default. See for information on how to modify this default value.

Group-Based SNMP Access



Note Because group is a standard SNMP term used industry-wide, roles are referred as groups in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

High Availability

Stateless restarts for SNMP are supported. After a reboot or supervisor switchover, the running configuration is applied.

Guidelines and Limitations for SNMP

- Read-only access to some SNMP MIBs is supported. See the Cisco NX-OS MIB support list at the following URL for more information:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
- SNMP role based access control (RBAC) is not supported.
- The SNMP set command is supported by the following Cisco MIBs:
 - CISCO-IMAGE-UPGRADE-MIB
 - CISCO-CONFIG-COPY-MIB
- The recommended SNMP polling interval time is 5 minutes.

Default Settings for SNMP

Parameters	Default
license notifications	enabled

Configuring SNMP

Configuring SNMP Users

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Places you in global configuration mode.
Step 2	switch(config)# snmp-server user name [auth {md5 sha} passphrase [auto] [priv	Configures an SNMP user with authentication and privacy parameters. The <i>passphrase</i> can be any case-sensitive, alphanumeric string up to 64 characters. If you use the localizekey

	Command or Action	Purpose
	[aes-128] <i>passphrase</i> [engineID <i>id</i>] [localizedkey]	<p>keyword, the <i>passphrase</i> can be any case-sensitive, alphanumeric string up to 130 characters.</p> <p>The <i>name</i> argument is the name of a user who can access the SNMP engine.</p> <p>The auth keyword enables one-time authentication for SNMP over a TCP session. It is optional.</p> <p>The md5 keyword specifies HMAC MD5 algorithm for authentication. It is optional.</p> <p>The sha keyword specifies HMAC SHA algorithm for authentication. It is optional.</p> <p>The priv keyword specifies encryption parameters for the user. It is optional.</p> <p>The aes-128 keyword specifies a 128-byte AES algorithm for privacy. It is optional.</p> <p>The engineID keyword specifies the engineID for configuring the notification target user (for V3 informs). It is optional.</p> <p>The <i>id</i> is a 12-digit colon-separated decimal number.</p>
Step 3	switch(config-callhome)# show snmp user	(Optional) Displays information about one or more SNMP users.
Step 4	switch(config-callhome)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
switch(config)#configure terminal
switch(config)# snmp-server user Admin auth sha Ax1m1234# priv Ax1m1234#
switch(config)# show snmp user
```

```
SNMP USERS
```

```
User Auth Priv(enforce) Groups
Admin sha des(no) network-operator
admin md5 des(no) network-admin
```

```
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
```

```
User Auth Priv
switch(config)#
```

Enforcing SNMP Message Encryption for All Users

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server community <i>name</i> {ro rw}	Creates an SNMP community string.

Filtering SNMP Requests

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message. The ACL applies to IPv4 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community. For more information on creating ACLs, see the Nexus 1000V for Microsoft Hyper-V Security Configuration Guide.

Use the following commands in global configuration mode to assign an ACL to a community to filter SNMP requests:

Before You Begin

Create an ACL to assign to the SNMP community. Assign the ACL to the SNMP community. Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source Port
- Destination Port

- Protocol (UDP or TCP)

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# ip access-list acl_for_community	Creates the named access list or places you in configuration mode for the specified access list.
Step 3	switch(config-acl)# statistics per-entry	Configures statistics.
Step 4	switch(config-acl)# permit udp any any	Permits UDP protocol.
Step 5	switch(config-acl)# show ip access-lists	(Optional) Displays show command output.
Step 6	switch(config-acl)# exit	Exits the current configuration mode.
Step 7	switch(config)# snmp community community-name	Configures SNMP community.
Step 8	switch(config)# snmp community community-name use-acl acl-name	Assigns an ACL to an SNMP community to filter SNMP requests.
Step 9	switch(config)# show snmp community	(Optional) Displays show command output.

```

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list acl_for_community
switch(config-acl)# statistics per-entry
switch(config-acl)# permit udp any any
switch(config-acl)# show ip access-lists

IPV4 ACL acl_for_community
    statistics per-entry
    10 permit udp any any [match=0]

switch(config-acl)# exit
switch(config)# snmp community public
switch(config)# snmp community public use-acl acl_for_community
switch(config)# show snmp community
SNMP_svrl                network-operator
public                    network-operator                acl_for_community

switch(config)#

```

Configuring SNMP Notification Receivers

Configuring a Host Receiver for SNMPv1 Traps

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server host <i>ip-address traps version 1 community</i> [udp_port number]	Configures a host receiver for SNMPv1 traps. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Configuring a Host Receiver for SNMPv2c Traps or Informs

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server host <i>ip-address {traps informs} version 2c</i> <i>community [udp_port number]</i>	Configures a host receiver for SNMPv2c traps or informs. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Configuring a Host Receiver for SNMPv3 Traps or Informs



Note

The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco device to authenticate and decrypt the SNMPv3 messages

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server host <i>ip-address</i> {traps informs} version 3 {auth noauth priv} <i>username</i> [udp_port <i>number</i>]	Configures a host receiver for SNMPv2c traps or informs. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth Admin
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
192.0.2.1 162 v3 auth inform Admin
-----
switch(config)#
```

Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver

The Cisco uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

**Note**

For authenticating and decrypting the received INFORM PDU, the notification host receiver should have the same user credentials as configured in Cisco NX-OS to authenticate and decrypt the inform s

Before You Begin

You must be in global configuration mode to configure the notification target user.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server user <i>name</i> [auth {md5 sha} <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i>] [engineID <i>id</i>]	Configures the notification target user with the specified engine ID for notification host receiver. The <i>id</i> is a 12-digit colon-separated decimal number.
	Example:	

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco enables all notifications. The following table lists the commands that enable the notifications for Cisco MIBs.


Note

The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

MIB	Related Commands
All notifications	snmp-server enable traps
CISCO-AAA-SERVER-MIB	snmp-server enable traps aaa
ENTITY-MIB	snmp-server enable traps entity
CISCO-ENTITY-FRU-CONTROL-MIB	snmp-server enable traps entity fru
CISCO-LICENSE-MGR-MIB	snmp-server enable traps license
IF-MIB	snmp-server enable traps link
SNMPv2-MIB	snmp-server enable traps snmp snmp-server enable traps snmp authentication

The license notifications are enabled by default. All other notifications are disabled by default.

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server enable traps	Enables all SNMP notifications.
Step 2	switch(config)# snmp-server enable traps aaa [server-state-change]	Enables the AAA SNMP notifications.
Step 3	switch(config)# snmp-server enable traps entity [fru]	Enables the ENTITY-MIB SNMP notifications.
Step 4	switch(config)# snmp-server enable traps license	Enables the license SNMP notification.
Step 5	switch(config)# snmp-server enable traps link	Enables the link SNMP notifications.

	Command or Action	Purpose
Step 6	switch(config)# snmp-server enable traps snmp [authentication]	Enables the SNMP agent notifications.

```
switch(config)# snmp-server enable traps

switch(config)# snmp-server enable traps aaa
switch(config)# snmp-server enable traps entity
switch(config)# snmp-server enable traps license
switch(config)# snmp-server enable traps link
switch(config)# snmp-server enable traps snmp
```

Disabling LinkUp/LinkDown Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use this limit notifications on flapping interface (an interface that transitions between up and down repeatedly).

Before You Begin

You must be in interface configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config-if)# no snmp trap link-status	Disables SNMP link-state traps for the interface. This command is enabled by default.

Enabling a One-time Authentication for SNMP over TCP

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server tcp-session [auth]	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server tcp-session
switch(config)# show snmp | grep "Tcp"
```

```
SNMP Tcp Authentication Flag : Enabled.
switch(config)#
```

Assigning the SNMP Switch Contact and Location Information

You can assign the switch contact information, which is limited to 32 characters (without spaces) and the switch location.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# snmp-server contact <i>name</i>	Configures sysContact, which is the SNMP contact name.
Step 3	switch(config)# snmp-server location <i>name</i>	Configures sysLocation, which is the SNMP location.
Step 4	switch(config)# show snmp	(Optional) Displays information about one or more destination profiles.
Step 5	switch(config)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
HPV-VSM# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HPV-VSM(config)# snmp-server contact Admin
HPV-VSM(config)# snmp-server location Lab
HPV-VSM(config)# show snmp | grep sys
sys contact: Admin
sys location: Lab
HPV-VSM(config)#copy running-config startup-config
```

Disabling SNMP

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# no snmp-server protocol enable	Disables the SNMP protocol. This command is enabled by default.

Modifying the AAA Synchronization Time

You can modify how long Cisco NX-OS holds the synchronized user configuration.

Before You Begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# snmp-server aaa-user cache-timeout <i>seconds</i>	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.

```
switch(config)# snmp-server aaa-user cache-timeout 1200
```

Verifying the SNMP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show interface snmp-ifindex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show running-config snmp [all]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.
show snmp group	Displays SNMP roles.

Command	Purpose
show snmp session	Displays SNMP sessions.
show snmp trap	Displays the SNMP notifications enabled or disabled.
show snmp user	Displays SNMPv3 users.

MIBs

Following is information about the supported SNMP MIBs.
 To locate and download the MIBs, go to the following URL:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

- IF-MIB
- ENTITY-MIB
- CISCO-ENTITY-EXT-MIB-V1SMI
- CISCO-ENTITY-FRU-CONTROL-MIB
- BRIDGE-MIB
- CISCO-FLASH-MIB
- CISCO-SYSTEM-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-FEATURE-CONTROL-MIB
- CISCO-CDP-MIB
- CISCO-VIRTUAL-NIC-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSLOG-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- TCP-MIB
- UDP-MIB
- CISCO-PRIVATE-VLAN-MIB
- CISCO-SECURE-SHELL-MIB
- CISCO-IMAGE-UPGRADE-MIB
- CISCO-LICENSE-MGR-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SERVER-EXT-MIB
- CISCO-COMMON-MGMT-MIB

- CISCO-COMMON-ROLES-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-LAG-MIB
- CISCO-NOTIFICATION-CONTROL-MIB
- CISCO-NTP-MIB
- CISCO-RF-MIB
- CISCO-SMI
- CISCO-SNMP-TARGET-EXT-MIB
- NOTIFICATION-LOG-MIB
- IP-MIB
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2-MIB

Feature History for SNMP

Feature Name	Releases	Feature Information
SNMP	Release 5.2(1)SK1(2.1)	This feature was introduced.