SNMP Version 3

The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network. Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415. This module discusses the security features provided in SNMPv3 and describes how to configure the security mechanism to handle SNMP packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About SNMP Version 3

Security Features in SNMP Version 3

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with during transit.
- Authentication—Determines that the message is from a valid source.

- Encryption—Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. 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 used when handling an SNMP packet.

The table below describes the combinations of SNMPv3 security models and levels.

Table 1: SNMP Version 3 Security Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication.
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

SNMPv3 supports RFCs 1901 to 1908, 2104, 2206, 2213, 2214, and 2271 to 2275. For more information about SNMPv3, see *RFC 2570, Introduction to Version 3 of the Internet-standard Network Management Framework* (this document is not a standard).

Cisco-Specific Error Messages for SNMP Version 3

Simple Network Management Protocol Version 3 (SNMPv3) provides different levels of security. If an authentication or an authorization request fails, a descriptive error message appears to indicate what went wrong. These error messages comply with *RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

You can use the **snmp-server usm cisco** command to disable the descriptive messages, thus preventing malicious users from misusing the information shown in the error messages. The table below describes the Cisco-specific error messages shown when the **snmp-server usm cisco** command is used, and the table compares these messages with the corresponding RFC 3414-compliant error messages.

Table 2: Cisco-Specific Error Messages for SNMPv3

Configured Security Level	Security Level of Incoming SNMP Message	RFC 3414-Compliant Error Indication	Cisco-Specific Error Messages
noAuthNoPriv	noAuthNoPriv	No error	No error
	authNoPriv	unsupportedSecurityLevel	unknownUserName
	authPriv	unsupportedSecurityLevel	unknownUserName
authNoPriv	noAuthNoPriv	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with correct authentication password	No error	No error
	authNoPriv with incorrect authentication password	wrongDigests	unknownUserName
	authPriv	unsupportedSecurityLevel	unknownUserName
authPriv	noAuthNoPriv	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with correct authentication password	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with incorrect authentication password	AUTHORIZATION_ERROR	unknownUserName
	authPriv with correct authentication password and correct privacy password	No error	No error
	authPriv with correct authentication password and incorrect privacy password	No response	No response
	authPriv with incorrect authentication password and correct privacy password	wrongDigests	unknownUserName
	authPriv with incorrect authentication password and incorrect privacy password	wrongDigests	unknownUserName

Note If an SNMP user belonging to an SNMP group is not configured with the password or if the group security level is not the same as the user security level, the error shown is “AUTHORIZATION_ERROR”. The Cisco-specific error message for this scenario is “unknownUserName”.

How to Configure SNMP Version 3

To configure the Simple Network Management Protocol Version 3 (SNMPv3) security mechanism and to use it to handle SNMP packets, you must configure SNMP groups and users with passwords.

Configuring the SNMP Server

To configure an SNMP server user, specify an SNMP group or a table that maps SNMP users to SNMP views. Then, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID by using the **snmp-server engineID** command for the remote agent. The SNMP engine ID of the remote agent is required to compute the authentication or privacy digests for the SNMP password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For SNMP notifications such as inform requests, the authoritative SNMP agent is the remote agent. You must configure the SNMP engine ID of the remote agent in the SNMP database before you can send proxy requests or inform requests to it.

Note The SNMP user cannot be removed if the engine ID is changed after configuring the SNMP user. To remove the user, you must first reconfigure all the SNMP configurations.

Note Default values do not exist for authentication or privacy algorithms when you configure the SNMP commands. Also, no default passwords exist. The minimum length for a password is one character, although it is recommended to use at least eight characters for security. If you forget a password, you cannot recover it and must reconfigure the user. You can specify either a plain text password or a localized MD5 digest.

Perform this task to specify an SNMP server group name and to add a new user to an SNMP group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*]
4. **snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*}
5. **snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*] **Example:** `Device(config)# snmp-server group group1 v3 auth access lmnop`	Configures the SNMP server group to enable authentication for members of a specified named access list. • In this example, the SNMP server group group1 is configured to enable user authentication for members of the named access list lmnop.
Step 4	**snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*} **Example:** `Device(config)# snmp-server engineID remote 172.16.15.4 udp-port 120 1a2833c0129a`	Configures the SNMP engine ID. • In this example, the SNMP engine ID is configured for a remote user.
Step 5	**snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]	Adds a new user to an SNMPv3 group and configures a plain text password for the user. **Note** For the *auth-password* argument, the minimum length is one character; the recommended length is at least eight characters, and the password should include both letters and numbers.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server user user1 group1 v3 auth md5 password123`	**Note** If you have the localized MD5 or SHA digest, you can specify the digest instead of the plain text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, cc, and dd are hexadecimal values. Also, the digest should be exactly 16 octets in length.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Verifying SNMP Version 3

Perform this task to verify the Simple Network Management Protocol Version 3 (SNMPv3) configuration. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show snmp group**
3. **show snmp user** [*username*]
4. **show snmp engineID**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show snmp group**
	Example:
	`Device# show snmp group`
	`groupname: V1 security model:v1`
	`readview : v1default writeview: <no writeview specified>`
	`notifyview: <no notifyview specified>`
	`row status: active`
	`groupname: ILMI security model:v1`
	`readview : *ilmi writeview: *ilmi`
	`notifyview: <no notifyview specified>`
	`row status: active`
		Displays information about each SNMP group in the network.
		Displays information about each SNMP group in the network.

	Command or Action	Purpose

	`groupname: ILMI security model:v2c`
	`readview : *ilmi writeview: *ilmi`
	
	`notifyview: <no notifyview specified>`
	`row status: active`
	`groupname: group1 security model:v1`
	`readview : v1default writeview: <no writeview specified>`
	`notifyview: <no notifyview specified>`
	`row status: active`	

Step 3	**show snmp user** [*username*]
	
	Example:
	
	`Device# show snmp user user1`
	
	`User name: user1`
	`Engine ID: 000000090200000000C025808`
	`storage-type: nonvolatile active access-list: 10`
	`Rowstatus: active`
	`Authentication Protocol: MD5`
	`Privacy protocol: DES`
	`Group name: group1`
		Displays information about configured characteristics of an SNMP user.

Step 4	**show snmp engineID**
	
	Example:
	`Device# show snmp engineID`
	
	`Local SNMP engineID: 1A2836C0129A`
	`Remote Engine ID IP-addr Port`
	`1A2833C0129A remote 10.2.28.1 120`
		Displays information about the SNMP engine ID that is configured for an SNMP user.

Configuration Examples for SNMP Version 3

Example: Configuring SNMP Version 3

The following example shows how to enable Simple Network Management Protocol Version 3 (SNMPv3). The configuration permits any SNMP manager to access all objects with read-only permissions using the community string named “public”. This configuration does not cause the device to send traps.

```
Device(config)# snmp-server community public
```

The following example shows how to configure a remote user to receive traps at the “noAuthNoPriv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group1 v3 noauth
Device(config)# snmp-server user remoteuser1 group1 remote 10.12.8.4
Device(config)# snmp-server host 10.12.8.4 informs version 3 noauth remoteuser config
```

The following example shows how to configure a remote user to receive traps at the “authNoPriv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group2 v3 auth
Device(config)# snmp-server user AuthUser group2 remote 10.12.8.4 v3 auth md5 password1
```

The following example shows how to configure a remote user to receive traps at the “priv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group3 v3 priv
Device(config)# snmp-server user PrivateUser group3 remote 10.12.8.4 v3 auth md5 password1
 priv access des56
```

Additional References for SNMP Version 3

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS SNMP Support Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 2570	*Introduction to Version 3 of the Internet-standard Network Management Framework*
RFC 2576	*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
RFC 3413	*SNMPv3 Applications*
RFC 3414	*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 3415	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

MIBs

MIB	MIBs Link
SNMP-COMMUNITY-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SNMP Version 3

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for SNMP Version 3

Feature Name	Releases	Feature Information
SNMP Version 3	12.0(6)S 15.0(1)S 15.4(1)S	The SNMP Version 3 feature is used to provide secure access to devices by authenticating and encrypting data packets over the network.