AES and 3-DES Encryption Support for SNMP Version 3

First Published: May 2005
Last Updated: June 5, 2007

The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of SNMP version 3. Data Encryption Standard (DES) support was introduced in Cisco IOS Release 12.0 and expanded in Cisco IOS Release 12.1. This support for Simple Network Management Protocol (SNMP) version 3 User-Based Security Model (USM) is complaint with RFC 3414, which defines DES as the only required method of message encryption for SNMP version 3 authPriv mode.

The AES and 3-DES Encryption Support for SNMP Version 3 feature adds Advanced Encryption Standard (AES) 128-bit encryption in compliance with RFC 3826. RFC 3826 extensions have been included in the SNMP-USM-AES-MIB. In addition, Cisco-specific extensions to support Triple-Data Encryption Algorithm (3-DES) and AES 192-bit and 256-bit encryption have been added to the CISCO-SNMP-USM-MIB. Additional information can be found in the Internet-Draft titled *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode* that can be found at the following URL: http://www.snmp.com/eso/draft-reeder-snmpv3-usm-3desede-00.txt.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for AES and 3-DES Encryption Support for SNMP Version 3" section on page 14.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for AES and 3-DES Encryption Support for SNMP Version 3

- The network management station (NMS) must support SNMP version 3 to use this feature of the SNMP agent.
- This feature is available in only Cisco IOS software images where encryption algorithms are supported.

Information About AES and 3-DES Encryption Support for SNMP Version 3

To configure the AES and 3-DES Encryption Support for SNMP Version 3 feature, you should understand the following concepts:

SNMP Architecture

The architecture for describing Internet Management Frameworks contained in RFC 3411 describes the SNMP engine as composed of the following components:

- Dispatcher
- Message Processing Subsystem
- Security Subsystem
- Access Control Subsystem

Applications make use of the services of these subsystems. It is important to understand the SNMP architecture and the terminology of the architecture to understand where the Security Model fits into the architecture and interacts with the other subsystems within the architecture. The information is contained in RFC 3411 and your are encouraged to review this RFC to obtain an understanding of the SNMP architecture and subsystem interactions.

Encryption Key Support

In the AES and 3-DES Encryption Support for SNMP Version 3 feature the Cipher Block Chaining/Data Encryption Standard (CBC-DES) is the privacy protocol. Originally only DES was supported (as per RFC 3414). This feature adds support for AES-128 (as per RFC 3826) and AES-192, AES-256 and 3-DES (as per CISCO-SNMP-USM-OIDS-MIB).

- AES encryption uses the Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits.
- 3DES encryption uses the 168-bit key size for encryption.

The AES Cipher Algorithm in the SNMP User-based Security Model draft describes the use of AES with 128-bit key size. However, the other options are also implemented with the extension to use the USM. There is currently no standard for generating localized keys for 192- or 256-bit size keys for AES or for 168-bit size key for 3-DES. There is no authentication protocol available with longer keys.

Management Information Base Support

The AES and 3-DES Encryption Support for SNMP Version 3 feature supports the selection of privacy protocols through the CLI and the Management Information Base (MIB). A new standard MIB, SNMP-USM-AES-MIB, provides support for the 128-bit key in AES. The extended options of AES with 192- or 256-bit keys and 3-DES are supported as extensions to the SNMP-USM-MIB, in the Cisco-specific MIB, CISCO-SNMP-USM-EXT-MIB.

How to Configure AES and 3-DES Encryption Support for SNMP Version 3

This section contains the following procedures:

- Adding a New User to an SNMP Group, page 3
- Verifying SNMP User Configuration, page 5

Adding a New User to an SNMP Group

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}] **Example:** `Router(config)# snmp-server user new-user new-group v3 auth md5 secureone priv aes 128 privatetwo 2`	Adds an SNMP user, specifies a group to which the user belongs, specifies the authorization algorithm to be used (MD5 or SHA), specifies the privacy algorithm to be used (DES, 3-DES, AES, AES-192, or AES-256), and specifies the password to be associated with this privacy protocol.

Verifying SNMP User Configuration

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the show snmp user command in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **show snmp user** *name*

Note The **show snmp user** command displays all the users configured on the router. However, unlike other snmp configurations, the **snmp-server user** command will not appear on the "show running" output.

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode. Enter your password when prompted.

Step 2 **show snmp user** *name*

The following example specifies the username as abcd, the engine ID string as 00000090200000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user abcd

User name: abcd
Engine ID: 00000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName


Group name: VacmGroupName
```

Additional References

The following sections provide references related to the AES and 3-DES Encryption Support for SNMP Version 3 feature.

Related Documents

Related Topic	Document Title
SNMP configuration tasks	*Cisco IOS Network Management Configuration Guide,* Release 12.4
SNMP commands	*Cisco IOS Network Management Command Reference,* Release 12.4T

Standards

Standard	Title
draft-reeder-snmpv3-usm-3desede-00.txt	*Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode*

MIBs

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

RFCs

RFC	Title
RFC 2574	*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 3411	*Architecture for Describing Internet Management Frameworks*
RFC 3414	*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 3826	*The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **show snmp user**
- **snmp-server user**

show snmp user

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the **show snmp user** command in privileged EXEC mode.

show snmp user [*username*]

Syntax Description

username	(Optional) Name of a specific user or users about which to display SNMP information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	The *username* argument was added. The output for this command was enhanced to show the authentication protocol (MD5 or SHA) and group name.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** *username group-name* command.

When the *username* argument is not entered, the **show snmp user** command displays information about all configured users. If you specify the *username* argument, if one or more users of that name exists, the information pertaining to those users is displayed. Because this command displays users configured with the SNMP engine ID of the local agent and other engine IDs, there can be multiple users with the same username.

When configuring SNMP, you may see the logging message “Configuring snmpv3 USM user.” USM stands for the User-based Security Model for version 3 of the Simple Network Management Protocol (SNMPv3). For further information on the USM, see RFC 2574.

Examples

The following is sample output from the **show snmp user** command. The output indicates the username as authuser, the engine ID string as 00000090200000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user authuser

User name: authuser
Engine ID: 00000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

Table 1 describes the significant fields shown in the display.

Table 1 show snmp user Field Descriptions

Field	Description
User name	A string identifying the name of the SNMP user.
Engine ID	A string identifying the name of the copy of SNMP on the device.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again.
active access-list	Standard IP access list associated with the SNMP user.
Rowstatus	Indicates whether Rowstatus is active or inactive.
Authentication Protocol	Identifies which authentication protocol is used. Options are message digest algorithm 5 (MD5), Secure Hash Algorithm (SHA) packet authentication, or None. • If authentication is not supported in your software image, this field will not be displayed.
Privacy protocol	Indicates whether Data Encryption Standard (DES) packet encryption is enabled. • If DES is not supported in your software image, this field will not be displayed.
Group name	Indicates the SNMP group the user is a part of. • SNMP groups are defined in the context of a View-based Access Control Model (VACM).

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*]
[**priv** {**des** | **3des** | **aes** {**128 | 192 |256**}} *privpassword*] {*acl-number* | *acl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*]]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*]
[**priv** {**des** | **3des** | **aes** {**128 | 192 |256**}} *privpassword*] {*acl-number* | *acl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
port	(Optional) Integer value that identifies the UDP port.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** or **auth** keywords or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an access control list (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user. Either IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
nacl	(Optional) Name of the ACL.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.

aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default

See Table 2 in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	Support for named standard access lists was added.
12.0(27)S	The **ipv6** *nacl* keyword/argument pair was added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
12.3(14)T	The **ipv6** *nacl* keyword/argument pair to allow for configuration of IPv6 named access lists and IPv6 remote hosts was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To configure a remote user, 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, using the **snmp-server engineID** command with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password* arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

Table 2 describes the default user characteristics for encryption, passwords, and access lists.

Table 2 snmp-server user Default Descriptions

Characteristic	Default
encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are MD5 digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized message digest 5 (MD5) digest.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the public SNMP server group. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Router(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the public group. In this example, access rules from the standard named access list qrst apply to the user.

```
Router(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password "cisco123" is configured for the user "abcd" in the SNMPv3 group "public":

```
Router(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, type the **show snmp user** command.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain text password:

```
Router(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user “abcd” is removed from the SNMP group “public”:

```
Router(config)# no snmp-server user abcd public v2c
```

In the following example, the user “abcd” from the SNMP group “public” specifies the use of the 168-bit 3DES algorithm for privacy encryption with “secure3des” as the password.

```
Router(config)# snmp-server user abcd public priv 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.

Feature Information for AES and 3-DES Encryption Support for SNMP Version 3

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for AES and 3-DES Encryption Support for SNMP Version 3

Feature Name	Releases	Feature Information
AES and 3-DES Encryption Support for SNMP Version 3	12.4(2)T 12.2(33)SRB	The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of SNMP version 3. DES support was introduced in Cisco IOS Release 12.0 and expanded in Cisco IOS Release 12.1. This support for SNMP version 3 USM is complaint with RFC 3414, which defines DES as the only required method of message encryption for SNMP version 3 authPriv mode. The AES and 3-DES Encryption Support for SNMP Version 3 feature adds AES 128-bit encryption in compliance with RFC 3826. AES and 3-DES Encryption Support for SNMP Version 3 was introduced in Cisco IOS Release 12.4(2)T. AES and 3-DES Encryption Support for SNMP Version 3 was integrated into Cisco IOS Release 12.2(33)SRB.