AES and 3-DES Encryption Support for SNMP Version 3

First Published: May 2005
Last Updated: February 28, 2009

The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of SNMP version 3. 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,* which can be found at the following URL: http://www.snmp.com/eso/draft-reeder-snmpv3-usm-3desede-00.txt.

Finding Feature Information

For the latest feature information and caveats, see 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 for AES and 3-DES Encryption Support for SNMP Version 3" section on page 7.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE 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, page 2
- Information About AES and 3-DES Encryption Support for SNMP Version 3, page 2
- How to Configure AES and 3-DES Encryption Support for SNMP Version 3, page 3
- Additional References, page 5
- Feature Information for AES and 3-DES Encryption Support for SNMP Version 3, page 7

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 Cisco IOS XE 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, page 2
- Encryption Key Support, page 3
- Management Information Base Support, page 3

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-OIDS-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 4

Adding a New User to an SNMP Group

SUMMARY STEPS

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

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*]} [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] [**access** [**ipv6** *nacl*] {*acl-number* | *acl-name*}] **Example:** `Router(config)# snmp-server user new-user new-group v3 auth md5 secureone priv aes 128 privatetwo access 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** [*username*]

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** [*username*]

The following example specifies the username as abcd, the engine ID string as 00000009020000000C025808, and the storage type as nonvolatile:

```
Router# show snmp user abcd

User name: abcd
Engine ID: 00000009020000000C025808
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 commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Cisco IOS XE commands	For information about Cisco IOS XE commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

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 XE 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. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

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

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE 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 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 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	Cisco IOS XE Release 2.1	The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of SNMP version 3. 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. The following commands were introduced or modified by this feature: **show snmp user**, **snmp-server user**