AES and 3-DES Encryption Support for SNMP Version 3

The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of Simple Network Management Protocol (SNMP) Version 3.

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.

- Finding Feature Information, page 1
- Prerequisites for AES and 3-DES Encryption Support for SNMP Version 3, page 1
- 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 4
- Additional References , page 6
- Feature Information for AES and 3-DES Encryption Support for SNMP Version 3, page 7

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.

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

- The network management station (NMS) must support Simple Network Management Protocol (SNMP) Version 3 to be able to use this feature.

- This feature is available only in Cisco software images that support encryption algorithms.
- It is important to understand the SNMP architecture and the terminology of the architecture to understand the security model used and how the security model interacts with the other subsystems in the architecture.

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

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

The encryption key sizes are:

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

The AES Cipher Algorithm in the Simple Network Management Protocol (SNMP) User-based Security Model (USM) 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 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 for longer keys.

Support for SNMP Version 3 USM is compliant 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 supports the selection of privacy protocols through the CLI and the MIB. A new standard MIB, SNMP-USM-AES-MIB, provides support for the 128-bit key in the Advanced Encryption Standard (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.

AES and 3-DES Encryption Support Overview

Each Simple Network Management Protocol (SNMP) entity includes a single SNMP engine. An SNMP engine implements functions for sending and receiving messages, authenticating and encrypting/decrypting messages, and controlling access to managed objects. These functions are provided as services to one or more applications that are configured with the SNMP engine to form an SNMP entity. The RFC 3411 describes the SNMP engine as composed of the following components:

- Dispatcher
- Message Processing Subsystem
- Security Subsystem

- Access Control Subsystem

Cipher Block Chaining/Data Encryption Standard (CBC-DES) is the privacy protocol for the AES and 3-DES Encryption Support for SNMP Version 3 feature. Prior to the introduction of this feature, 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). 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.

The encryption key sizes are:

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

The AES Cipher Algorithm in the Simple Network Management Protocol (SNMP) User-based Security Model (USM) 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 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 for longer keys.

Support for SNMP Version 3 USM is compliant 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 supports the selection of privacy protocols through the CLI and the MIB. A new standard MIB, SNMP-USM-AES-MIB, provides support for the 128-bit key in the Advanced Encryption Standard (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.

Encryption Key Support

MIB Support

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

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*}]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Device# 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:** `Device(config)# snmp-server user new-user`	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.

	Command or Action	Purpose
	`new-group v3 auth md5 secureone priv aes 128 privatetwo access 2`	
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the 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.

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

SUMMARY STEPS

1. **enable**
2. **show snmp user** [*username*]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enters privileged EXEC mode. Enter your password when prompted.

Step 2 **show snmp user** [*username*]

Example:

```
Device# show snmp user abcd

User name: abcd
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName
Group name: VacmGroupName
```

The above example specifies the username as abcd, the engine ID string as 000000090200000000C025808, and the storage type as nonvolatile:

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
commands	

Standards

Standard	Title

MIBs

MIB	MIBs Link
	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

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