



AES and 3-DES Encryption Support for SNMP Version 3

First Published: May 2005
Last Updated: November 8, 2010

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 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 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

Your software release may not support all the features documented in this module. 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 software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



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 only Cisco IOS software images where encryption algorithms are supported.

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

- [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 you 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 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*] [**vrf** *vrf-name*]]
{ **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** [**ipv6** *nacl*]
{ **priv** { **des** | **3des** | **aes** { **128** | **192** | **256** } } *privpassword*] { *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 <i>username group-name</i> [remote <i>host</i> [udp-port <i>port</i>][vrf <i>vrf-name</i>]] { v1 v2c v3 [encrypted] [auth { md5 sha } <i>auth-password</i>]} [access [ipv6 <i>nacl</i>] [priv { des 3des aes { 128 192 256 }} <i>privpassword</i>] [<i>acl-number</i> <i>acl-name</i>]] 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** [*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

### Related Documents

| Related Topic            | Document Title                                                   |
|--------------------------|------------------------------------------------------------------|
| Cisco IOS commands       | <a href="#">Cisco IOS Master Commands List, All Releases</a>     |
| SNMP commands            | <a href="#">Cisco IOS Network Management Command Reference</a>   |
| SNMP configuration tasks | <a href="#">Cisco IOS Network Management Configuration Guide</a> |

### Standards

| Standard                              | Title                                                                                                            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------|
| draft-reeder-snmv3-usm-3desede-00.txt | <a href="#">Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in “Outside” CBC Mode</a> |

### MIBs

| MIB                                                                                                 | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>CISCO-SNMP-USM-OIDS-MIB</li> <li>SNMP-USM-AES-MIB</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

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

## 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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# 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 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 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.

**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 | 12.2(33)SRB<br>12.2(33)SB<br>12.2(33)SXI<br>12.4(2)T<br>15.0(1)S<br>Cisco IOS XE<br>3.1.0SG | <p>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 compliant with RFC 3414, which defines DES as the only required method of message encryption for SNMP version 3 authPriv mode.</p> <p>The AES and 3-DES Encryption Support for SNMP Version 3 feature adds AES 128-bit encryption in compliance with RFC 3826.</p> <p>AES and 3-DES Encryption Support for SNMP Version 3 was introduced in Cisco IOS Release 12.4(2)T.</p> <p>AES and 3-DES Encryption Support for SNMP Version 3 was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>AES and 3-DES Encryption Support for SNMP Version 3 was integrated into Cisco IOS Release 12.2(33)SB.</p> <p>This feature was integrated into Cisco IOS Release 15.0(1)S.</p> |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2010 Cisco Systems, Inc. All rights reserved.

