AES-CTR Support for SSHv2

The AES-CTR Support for SSHv2 feature provides increased security through support for the Advanced Encryption Standard counter (AES-CTR) encryption mode during an encrypted Secure Shell version 2 (SSHv2) session between the server and the client.

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 at the end of this module.

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-CTR Support for SSHv2

- Ensure that you use a Secure Shell (SSH) remote device that supports SSH Version 2 (SSHv2) and connect to a Cisco device.
- Ensure that both the client and the server that are used in the SSH session support the Advanced Encryption Standard counter mode (AES-CTR) encryption mode.

Restrictions for AES-CTR Support for SSHv2

- The Secure Shell (SSH) server and SSH client are supported only on crypto k9 (Triple Data Encryption Standard [3DES]) software images depending on your release.

Information About AES-CTR Support for SSHv2

Secure Shell Version 2 Encryption Modes

The Cisco Secure Shell (SSH) implementation enables a secure, encrypted connection between a server and client. The SSH servers and clients use the SSH protocol to provide device authentication and encryption.

To start an encrypted session between the SSH client and server, the preferred mode of encryption needs to be decided. For increased security, the preferred crypto algorithm for the SSH session is the Advanced Encryption Standard counter mode (AES-CTR).

SSH version 2 (SSHv2) supports AES-CTR encryption for 128-, 192-, and 256-bit key length. From the supported AES-CTR algorithms, the preferred algorithm is chosen based on the processing capability. The greater the length of the key, the stronger the encryption.

The Cisco SSH servers and clients support three types of crypto algorithms to encrypt data and selects the encryption mode in the following order of preferred encryption:

- AES-CTR
- AES Cipher Block Chaining (AES-CBC)
- Triple Data Encryption Standard (3DES)

If the SSH session uses a remote device that does not support the AES-CTR encryption mode, then the encryption mode for the session falls back to AES-CBC mode.

How to Configure AES-CTR Support for SSHv2

Starting an Encrypted Session from the SSH Client

Perform this task to start an encrypted Secure Shell (SSH) session from the SSH client using the Advanced Encryption Standard counter mode (AES-CTR) encryption mode.

Note The device with which you want to connect must support an SSH server that has the AES-CTR encryption algorithm that is supported in Cisco software. SSH can be run even when the device is disabled.

SUMMARY STEPS

1. **enable**
2. **ssh** [**-v** {**1** | **2**} | **-c** {**aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-cbc** | **3des** | **aes192-cbc** | **aes256-cbc**} | **-l** *user-id* | **-l** *user-id*:*vrf-name number ip-address ip-address* | **-l** *user-id*:*rotary number ip-address* | **-m** {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**} | **-o numberofpasswordprompts** *n* | **-p** *port-num*] {*ip-addr* | *hostname*} [**command** | **-vrf**]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ssh** [**-v** {**1**	**2**}	**-c** {**aes128-ctr**	**aes192-ctr**	**aes256-ctr**	**aes128-cbc**	**3des**	**aes192-cbc**	**aes256-cbc**}	**-l** *user-id*	**-l** *user-id*:*vrf-name number ip-address ip-address*	**-l** *user-id*:*rotary number ip-address*	**-m** {**hmac-md5-128**	**hmac-md5-96**	**hmac-sha1-160**	**hmac-sha1-96**}	**-o numberofpasswordprompts** *n*	**-p** *port-num*] {*ip-addr*	*hostname*} [**command**	**-vrf**] **Example:** `Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24`	Starts an encrypted session with a remote networking device.
Step 3	**exit** **Example:** `Device# exit`	Exits privileged EXEC mode.

Verifying the Encryption Mode Used in the SSH Server or Client

SUMMARY STEPS

1. **enable**
2. **show ssh**
3. **debug ip ssh detail**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ssh**

Displays the encryption algorithms used for an encrypted session.

Example:

The following sample output from the **show ssh** command shows that the AES-CTR encryption mode is used for the session between the SSH server and client:

```
Device# show ssh

Connection Version Mode Encryption  Hmac                State         Username

0          1.99     IN   aes128-ctr  hmac-sha1     Session started       cisco
0          1.99     OUT  aes128-ctr  hmac-sha1     Session started       cisco

%No SSHv1 server connections running.
```

Step 3 **debug ip ssh detail**

Displays the version and configuration data for Secure Shell (SSH).

Example:

The following sample output from the **debug ip ssh detail** command in the SSH server shows that the AES-CTR encryption mode is used for the session between the SSH server and client:

```
Device# debug ip ssh detail

SSH2 0: kex: client->server enc:aes128-ctr mac:hmac-md5
SSH2 0: kex: server->client enc:aes128-ctr mac:hmac-md5
```

The following sample output from the **debug ip ssh detail** command in the SSH client shows that the AES-CTR encryption mode is used for the session between the SSH server and client:

```
Device# debug ip ssh detail

SSH2 CLIENT 0: kex: server->client enc:aes128-ctr mac:hmac-md5
SSH2 CLIENT 0: kex: client->server enc:aes128-ctr mac:hmac-md5
```

Configuration Examples for AES-CTR Support for SSHv2

Example: Starting an Encrypted Session from the SSH Client

The following example shows how to start an encrypted Secure Shell (SSH) session from the SSH client using the Advanced Encryption Standard counter mode (AES-CTR) encryption mode:

```
Device> enable
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24
Device# exit
```

Additional References for AES-CTR Support for SSHv2

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
SSH configuration	*Secure Shell Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 4344	*The Secure Shell (SSH) Transport Layer Encryption Modes*

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/cisco/web/support/index.html

Feature Information for AES-CTR Support for SSHv2

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-CTR Support for SSHv2

Feature Name	Releases	Feature Information
AES-CTR Support for SSHv2	15.4(2)T 15.2(1)SY	The AES-CTR Support for SSHv2 feature provides increased security through support for the Advanced Encryption Standard counter (AES-CTR) encryption mode during an encrypted Secure Shell version 2 (SSHv2) session between the server and the client.