



SSH Algorithms for Common Criteria Certification

- [Restriction for SSH Algorithms for Common Criteria Certification, on page 1](#)
- [Information About SSH Algorithms for Common Criteria Certification, on page 1](#)
- [How to Configure SSH Algorithms for Common Criteria Certification, on page 3](#)
- [Configuration Examples For SSH Algorithms for Common Criteria Certification, on page 7](#)
- [Verifying SSH Algorithms for Common Criteria Certification , on page 8](#)
- [Feature Information for Secure Shell Algorithms for Common Criteria Certification , on page 9](#)

Restriction for SSH Algorithms for Common Criteria Certification

Starting from Cisco IOS XE Amsterdam 17.1.1, SHA1 is not supported.

Information About SSH Algorithms for Common Criteria Certification

This section provides information about the Secure Shell (SSH) Algorithms for Common Criteria Certification, the Cisco IOS SSH Server Algorithms and Cisco IOS SSH Client Algorithms.

SSH Algorithms for Common Criteria Certification

A Secure Shell (SSH) configuration enables a Cisco IOS SSH server and client to authorize the negotiation of only those algorithms that are configured from the allowed list. If a remote party tries to negotiate using only those algorithms that are not part of the allowed list, the request is rejected and the session is not established.

Cisco IOS SSH Server Algorithms

Cisco IOS secure shell (SSH) servers support the encryption algorithms (Advanced Encryption Standard Counter Mode [AES-CTR], AES Cipher Block Chaining [AES-CBC], Triple Data Encryption Standard [3DES]) in the following order:

Supported Default Encryption Order:

1. aes128-gcm

2. aes256-gcm
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr

Supported Non-Default Encryption Order:

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc
4. 3des

Cisco IOS SSH clients support the Message Authentication Code (MAC) algorithms in the following order:

Supported Default HMAC order:

1. hmac-sha2-256
2. hmac-sha2-512

Cisco IOS SSH clients support only one host key algorithm and do not need a CLI configuration.

Supported Default Host Key order:

1. x509v3-ssh-rsa
2. ssh-rsa

Cisco IOS SSH Client Algorithms

Cisco IOS secure shell (SSH) clients support the encryption algorithms (Advanced Encryption Standard counter mode [AES-CTR], AES Cipher Block Chaining [AES-CBC], Triple Data Encryption Standard [3DES]) in the following order:

Supported Default Encryption Order:

1. aes128-gcm
2. aes256-gcm
3. aes128-ctr
4. aes192-ctr
5. aes256-ctr

Supported Non-Default Encryption Order:

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc

4. 3des

Cisco IOS SSH clients support the Message Authentication Code (MAC) algorithms in the following order:

Supported Default HMAC order:

1. hmac-sha2-256
2. hmac-sha2-512

Cisco IOS SSH clients support only one host key algorithm and do not need a CLI configuration.

Supported Default Host Key order:

1. x509v3-ssh-rsa
2. ssh-rsa

How to Configure SSH Algorithms for Common Criteria Certification

This section provides information on how to configure and troubleshoot:

- Encryption key algorithm for a Cisco IOS SSH server and client
- MAC algorithm for a Cisco IOS SSH server and client
- Host Key algorithm for a Cisco IOS SSH server

Configuring an Encryption Key Algorithm for a Cisco IOS SSH Server and Client

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip ssh {server client} algorithm encryption {aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc 3des-cbc } Example: | Defines the order of encryption algorithms in the SSH server and client. This order is presented during algorithm negotiation. Note The Cisco IOS SSH server and client must have at least one configured encryption algorithm. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <pre>Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc</pre> | <p>Note To disable one algorithm from the previously configured algorithm list, use the no form of this command. To disable more than one algorithm, use the no form of this command multiple times with different algorithm names.</p> <p>Note For a default configuration, use the default form of this command as shown below:</p> <pre>Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc</pre> |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Exits global configuration mode and returns to privileged EXEC mode. |

Troubleshooting Tips

If you try to disable the last encryption algorithm in the configuration, the following message is displayed and the command is rejected:

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

Configuring a MAC Algorithm for a Cisco IOS SSH Server and Client

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Device> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | <p>ip ssh {server client} algorithm mac {hmac-sha2-256 hmac-sha2-512 }</p> <p>Example:</p> <pre>Device(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512</pre> <pre>Device(config)# ip ssh client algorithm mac hmac-sha2-256 hmac-sha2-512</pre> | <p>Defines the order of MAC (Message Authentication Code) algorithms in the SSH server and client. This order is presented during algorithm negotiation.</p> <p>Note The Cisco IOS SSH server and client must have at least one configured Hashed Message Authentication Code (HMAC) algorithm.</p> <p>Note To disable one algorithm from the previously configured algorithm list, use the no form of this command. To disable more than one algorithm, use the no form of this command multiple times with different algorithm names.</p> <p>Note For default configuration, use the default form of this command as shown below:</p> <pre>Device(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512</pre> |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | <p>Exits global configuration mode and returns to privileged EXEC mode.</p> |

Troubleshooting Tips

If you try to disable the last MAC algorithm in the configuration, the following message is displayed and the command is rejected:

```
% SSH command rejected: All mac algorithms cannot be disabled
```

Configuring a Host Key Algorithm for a Cisco IOS SSH Server

Procedure

| | Command or Action | Purpose |
|---------------|-------------------|-------------------------------|
| Step 1 | enable | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Example: Device> enable | Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip ssh server algorithm hostkey {x509v3-ssh-rsa ssh-rsa} Example: Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa | Defines the order of host key algorithms. Only the configured algorithm is negotiated with the Cisco IOS secure shell (SSH) client. Note The Cisco IOS SSH server must have at least one configured host key algorithm: <ul style="list-style-type: none"> • x509v3-ssh-rsa—X.509v3 certificate-based authentication • ssh-rsa—Public-key-based authentication Note To disable one algorithm from the previously configured algorithm list, use the no form of this command. To disable more than one algorithm, use the no form of this command multiple times with different algorithm names. Note For default configuration, use the default form of this command as shown below: Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa |
| Step 4 | end Example: Device(config)# end | Exits global configuration mode and returns to privileged EXEC mode. |

Troubleshooting Tips

If you try to disable the last host key algorithm in the configuration, the following message is displayed and the command is rejected:

```
% SSH command rejected: All hostkey algorithms cannot be disabled
```

Configuration Examples For SSH Algorithms for Common Criteria Certification

This section provides configuration examples for SSH algorithms for common certification.

Example: Configuring Encryption Key Algorithms for a Cisco IOS SSH Server

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc
aes192-cbc aes256-cbc 3des
Device(config)# end
```

Example: Configuring Encryption Key Algorithms for a Cisco IOS SSH Client

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc
aes192-cbc aes256-cbc 3des

Device(config)# end
```

Example: Configuring MAC Algorithms for a Cisco IOS SSH Server

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512
Device(config)# end
```

Example: Configuring Host Key Algorithms for a Cisco IOS SSH Server

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa
Device(config)# end
```

Verifying SSH Algorithms for Common Criteria Certification

Procedure

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ip ssh**

Displays configured Secure Shell (SSH) encryption, host key, and Message Authentication Code (MAC) algorithms.

Example:

The following sample output from the **show ip ssh** command shows the encryption algorithms configured in the default order:

```
Device# show ip ssh
```

```
Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc  
3des
```

The following sample output from the **show ip ssh** command shows the MAC algorithms configured in the default order:

```
Device# show ip ssh
```

```
MAC Algorithms: hmac-sha2-256, hmac-sha2-512
```

The following sample output from the **show ip ssh** command shows the host key algorithms configured in the default order:

```
Device# show ip ssh
```

```
Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

Feature Information for Secure Shell Algorithms for Common Criteria Certification

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|---------------------------------|---|---|
| Cisco IOS XE Everest 16.5.1a | Secure Shell Algorithms for Common Criteria Certification | The SSH Algorithms for Common Criteria Certification feature provides the list and order of the algorithms that are allowed for Common Criteria Certification. This module describes how to configure the encryption, Message Authentication Code (MAC), and host key algorithms for a secure shell (SSH) server and client so that SSH connections can be limited on the basis of the allowed algorithms list. |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

