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 5
- Configuration Examples For SSH Algorithms for Common Criteria Certification, on page 10
- Verifying SSH Algorithms for Common Criteria Certification , on page 12
- Feature History for Secure Shell Algorithms for Common Criteria Certification , on page 12

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, and the priority of the algorithms are based on the user configuration. 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]), and Galois/Counter Mode (GCM) in the following order:

Supported Default Encryption Order:

1. chacha20-poly1305@openssh.com

2. aes128-gcm@openssh.com
3. aes256-gcm@openssh.com
4. aes128-gcm
5. aes256-gcm
6. aes128-ctr
7. aes192-ctr
8. aes256-ctr

Supported Non-Default Encryption:

- aes128-cbc
- aes192-cbc
- aes256-cbc
- 3des-cbc

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

Supported Default HMAC Order:

1. hmac-sha2-256-etm@openssh.com
2. hmac-sha2-512-etm@openssh.com

Supported Non-Default HMAC:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Cisco IOS SSH servers support the host key algorithms in the following order:

Supported Default Host Key Order:

1. rsa-sha2-512
2. rsa-sha2-256
3. ssh-rsa

Supported Non-Default Host Key:

- x509v3-ssh-rsa

Cisco IOS SSH servers support the Key Exchange (KEX) DH Group algorithms in the following default order:

Supported Default KEX DH Group Order:

1. curve25519-sha256

2. curve25519-sha256@libssh.org
3. ecdh-sha2-nistp256
4. ecdh-sha2-nistp384
5. ecdh-sha2-nistp521
6. diffie-hellman-group14-sha256
7. diffie-hellman-group16-sha512

Supported Non-Default KEX DH Group:

- diffie-hellman-group14-sha1

Cisco IOS SSH servers support the public key algorithms in the following default order:

Supported Default Public Key Order:

1. ssh-rsa
2. ecdsa-sha2-nistp256
3. ecdsa-sha2-nistp384
4. ecdsa-sha2-nistp521
5. ssh-ed25519
6. x509v3-ecdsa-sha2-nistp256
7. x509v3-ecdsa-sha2-nistp384
8. x509v3-ecdsa-sha2-nistp521
9. rsa-sha2-256
10. rsa-sha2-512
11. x509v3-rsa2048-sha256

Supported Non-Default Public Key:

- x509v3-ssh-rsa

Cisco IOS SSH Client Algorithms

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

Supported Default Encryption Order:

1. chacha20-poly1305@openssh.com
2. aes128-gcm@openssh.com
3. aes256-gcm@openssh.com

4. aes128-gcm
5. aes256-gcm
6. aes128-ctr
7. aes192-ctr
8. aes256-ctr

Supported Non-Default Encryption:

- aes128-cbc
- aes192-cbc
- aes256-cbc
- 3des-cbc

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

Supported Default HMAC order:

1. hmac-sha2-256-etm@openssh.com
2. hmac-sha2-512-etm@openssh.com

Supported Non-Default HMAC:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Cisco IOS SSH clients support the Key Exchange (KEX) DH Group algorithms in the following default order:

Supported Default KEX DH Group Order:

1. curve25519-sha256
2. curve25519-sha256@libssh.org
3. ecdh-sha2-nistp256
4. ecdh-sha2-nistp384
5. ecdh-sha2-nistp521
6. diffie-hellman-group14-sha256
7. diffie-hellman-group16-sha512

Supported Non-Default KEX DH Group:

- diffie-hellman-group14-sha1

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** {**3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes128-gcm@openssh.com** | **aes192-cbc** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **aes256-gcm@openssh.com** | **chacha20-poly1305@openssh.com**}
	Example:
	`Device(config)# ip ssh server algorithm encryption 3des-cbc aes128-cbc aes128-ctr aes128-gcm aes128-gcm@openssh.com aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-gcm aes256-gcm@openssh.com chacha20-poly1305@openssh.com`
	`Device(config)# ip ssh client algorithm encryption 3des-cbc aes128-cbc aes128-ctr aes128-gcm aes128-gcm@openssh.com aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-gcm aes256-gcm@openssh.com chacha20-poly1305@openssh.com`
		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.
		• 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.
		For a default configuration, use the default form of this command as shown below:
		`Device(config)# ip ssh server algorithm encryption chacha20-poly1305@openssh.com aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-gcm aes256-gcm aes128-ctr aes192-ctr`

	Command or Action	Purpose
		aes256-ctr `Device(config)# ip ssh client algorithm encryption chacha20-poly1305@openssh.com aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-gcm aes256-gcm aes128-ctr aes192-ctr aes256-ctr`
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 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	**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 mac** {**hmac-sha1** | **hmac-sha2-256** | **hmac-sha2-256-etm@openssh.com** | **hmac-sha2-512** | **hmac-sha2-512-etm@openssh.com**}
	Example:
	`Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm hmac-sha2-256 hmac-sha2-512`
	`Device(config)# ip ssh client algorithm mac hmac-sha2-256-etm hmac-sha2-512-etm hmac-sha2-256 hmac-sha2-512`
		Defines the order of MAC (Message Authentication Code) 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 Hashed Message Authentication Code (HMAC) algorithm.
		• 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.

	Command or Action	Purpose

		For default configuration, use the default form of this command as shown below:
		`Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com`
		`Device(config)# ip ssh client algorithm mac hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com`

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 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 Key Exchange DH Group Algorithm for 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 kex** {**curve25519-sha256** | **curve25519-sha256@libssh.org** | **diffie-hellman-group14-sha1** | **diffie-hellman-group14-sha256** | **diffie-hellman-group16-sha512** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384**|**ecdh-sha2-nistp521** } **Example:** `Device(config)# ip ssh server algorithm kex curve25519-sha256@libssh.org diffie-hellman-group14-sha1`	Defines the order of Key Exchange 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 KEX algorithm. • 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

	Command or Action	Purpose

	ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
	`Device(config)# ip ssh client algorithm kex curve25519-sha256@libssh.org diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521`
		of this command multiple times with different algorithm names.
		For default configuration, use the default form of this command as shown below:
		`Device(config)# ip ssh server algorithm kex curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512`
		`Device(config)# ip ssh client algorithm kex curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512`

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 KEX algorithm in the configuration, the following message is displayed and the command is rejected:

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

Configuring a Public Key Algorithm for a Cisco IOS SSH Server

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 algorithm publickey** {**ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **ecdsa-sha2-nistp521** | **rsa-sha2-256** | **rsa-sha2-512** | **ssh-ed25519** | **ssh-rsa** |	Defines the order of public key algorithms in the SSH server. This order is presented during algorithm negotiation. **Note**

	Command or Action	Purpose
	x509v3-ecdsa-sha2-nistp256 | **x509v3-ecdsa-sha2-nistp384** | **x509v3-ecdsa-sha2-nistp521** | **x509v3-rsa2048-sha256** | **x509v3-ssh-rsa**} **Example:** `Device(config)# ip ssh server algorithm publickey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 rsa-sha2-256 rsa-sha2-512 ssh-ed25519 ssh-rsa x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521 x509v3-rsa2048-sha256 x509v3-ssh-rsa`	• The Cisco IOS SSH server must have at least one configured public key algorithm. • 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. For default configuration, use the default form of this command as shown below: `Device(config)# ip ssh server algorithm publickey ssh-rsa ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521 rsa-sha2-256 rsa-sha2-512 x509v3-rsa2048-sha256`
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 public key algorithm in the configuration, the following message is displayed and the command is rejected:

```
% SSH command rejected: All public key algorithms cannot be disabled
```

Configuring a Host Key Algorithm for a Cisco IOS SSH Server

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 algorithm hostkey** {**rsa-sha2-512** | **rsa-sha2-256** | **ssh-rsa** | **x509v3-ssh-rsa**}	Defines the order of host key algorithms. Only the configured algorithm is negotiated with the Cisco IOS secure shell (SSH) server.

	Command or Action	Purpose
	Example: `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa rsa-sha2-512 rsa-sha2-256 ssh-rsa`	**Note** • The Cisco IOS SSH server must have at least one configured host key algorithm. • 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. For default configuration, use the default form of this command as shown below: `Device(config)# ip ssh server algorithm hostkey rsa-sha2-512 rsa-sha2-256 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 3des-cbc aes128-cbc aes128-ctr aes128-gcm
 aes128-gcm@openssh.com aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-
gcm aes256-gcm@openssh.com chacha20-poly1305@openssh.com
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 3des-cbc aes128-cbc aes128-ctr aes128-gcm
 aes128-gcm@openssh.com aes192-cbc aes192-ctr aes256-cbc aes256-ctr aes256-
gcm aes256-gcm@openssh.com chacha20-poly1305@openssh.com
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-sha1 hmac-sha2-256
hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm hmac-sha2-512-etm@openssh.com
Device(config)# end
```

Example: Configuring Key Exchange DH Group for a Cisco IOS SSH Server

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex ecdh-sha2-nistp256 ecdh-sha2-nistp384
ecdh-sha2-nistp521 diffie-hellman-group14-sha1 curve25519-sha256@libssh.org
Device(config)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm publickey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384
ecdsa-sha2-nistp521 rsa-sha2-256 rsa-sha2-512 ssh-ed25519 ssh-rsa x509v3-ecdsa-sha2-nistp256
 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521 x509v3-rsa2048-sha256 x509v3-ssh-rsa
Device(config)# end
```

The following example shows how to return to the default behavior in which all public key algorithms are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm publickey
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 rsa-sha2-512 rsa-sha2-256
ssh-rsaa
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 History for Secure Shell Algorithms for Common Criteria Certification

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

These features are available in all the 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.
Cisco IOS XE Cupertino 17.8.1	Secure Shell Encryption Algorithms	Cisco IOS SSH Server and Client support for the following encryption algorithms have been introduced: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly1305@openssh.com
Cisco IOS XE Cupertino 17.9.1	Secure Shell Encryption Algorithms	Cisco IOS SSH Server and Client support for the following encryption algorithms have been introduced: • aes128-gcm@openssh.com • aes256-gcm@openssh.com

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.