

Configuring SSH and Telnet

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on Cisco NX-OS devices.

This chapter includes the following sections:

- About SSH and telnet, on page 1
- Prerequisites for SSH and telnet, on page 3
- Guidelines and limitations for SSH and telnet, on page 3
- Default settings for SSH and telnet, on page 5
- Configuring SSH , on page 5
- Configuring telnet, on page 26
- SSH and telnet configuration verification commands, on page 28
- Configuration example for SSH, on page 29
- Configuration example for SSH passwordless file copy, on page 30
- Configuration example for x.509v3 Certificate-Based SSH authentication, on page 31
- Additional references for SSH and telnet, on page 32

About SSH and telnet

This section includes information about SSH and Telnet.

SSH server

You can use the SSH server to enable an SSH client to make a secure, encrypted connection to a Cisco NX-OS device. SSH uses strong encryption for authentication. The SSH server in the Cisco NX-OS software can interoperate with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, LDAP, and the use of locally stored usernames and passwords.

SSH client

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco NX-OS device to make a secure, encrypted connection to another Cisco NX-OS device or to any other device that runs the SSH server. This connection provides an outbound

connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco NX-OS software works with publicly and commercially available SSH servers.

SSH server keys

SSH requires server keys for secure communications to the Cisco NX-OS device. You can use SSH server keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algrorithm (DSA)
- SSH version 2 using the Elliptic Curve Digital Signature Algorithm (ECDSA)

Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts the following types of key-pairs for use by SSH version 2:

- The **dsa** option generates the DSA key-pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA key-pair for the SSH version 2 protocol.
- The **ecdsa** option generates the ECDSA key-pair for the SSH version 2 protocol.

By default, the Cisco NX-OS software generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)
- Public Key Certificate in Privacy-Enhanced Mail (PEM)



Caution If you delete all of the SSH keys, you cannot start the SSH services.

SSH authentication using digital certificates

SSH authentication on Cisco NX-OS devices provide X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through a query or a notification. Verification of certificates is successful if the certificates are from any of the trusted CAs configured and if not revoked or expired.

You can configure your device for SSH authentication using an X.509 certificate. If the authentication fails, you are prompted for a password.

You can configure SSH authentication using X.509v3 certificates (RFC 6187). X.509v3 certificate-based SSH authentication uses certificates combined with a smartcard to enable two-factor authentication for Cisco device access. The SSH client is provided by Cisco partner Pragma Systems.

Telnet server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

The Telnet server is disabled by default on the Cisco NX-OS device.

Post-quantum key exchange for SSH

Post-quantum key exchange for SSH is the key exchange phase used during SSH session establishment that

- derives per-connection keying material during SSH setup,
- uses post-quantum or hybrid key exchange algorithms to protect the shared secret, and
- negotiates a key exchange algorithm supported by both SSH peers.

Key exchange behavior

Hybrid key exchange combines a classical key exchange mechanism with a post-quantum mechanism. The resulting shared secret remains protected if at least one component remains secure.

PQC-only Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) options are available when both peers support the same ML-KEM algorithm.

SSH peers negotiate a mutually supported key exchange algorithm. If a peer does not support configured PQC or hybrid algorithms, the connection can fall back to a mutually supported classical key exchange algorithm only if classical algorithms remain enabled on both peers.

Prerequisites for SSH and telnet

Make sure that you have configured IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

Guidelines and limitations for SSH and telnet

Use this reference to review the guidelines and limitations for SSH and telnet.

SSH and Telnet have the following configuration guidelines and limitations:

- The Cisco NX-OS software supports only SSH version 2 (SSHv2).
- Beginning with Cisco NX-OS Release 10.4(3)F, the Cisco Nexus 9000 Series switches support SSH authorization using X.509 certificates through a TACACS+ server. This feature is not supported with RADIUS.

- When you use the **no feature ssh feature** command, port 22 is not disabled . Port 22 is always open and a deny rule is pushed to deny all incoming external connections.
- Due to a Poodle vulnerability, SSLv3 is no longer supported.
- IPSG is not supported on the following:
  - The last six 40-Gb physical ports on the Cisco Nexus 9372PX, 9372TX, and 9332PQ switches
  - All 40G physical ports on the Cisco Nexus 9396PX, 9396TX, and 93128TX switches
- You can configure your device for SSH authentication using an X.509 certificate. If the authentication fails, you are prompted for a password.
- The SFTP server feature does not support the regular SFTP **chown** and **chgrp** commands.
- When the SFTP server is enabled, only the admin user can use SFTP to access the device.

SSH key persistence, timeout, and command display limitations

- SSH public and private keys imported into user accounts that are remotely authenticated through a AAA protocol (such as RADIUS or TACACS+) for the purpose of SSH Passwordless File Copy will not persist when the Nexus device is reloaded unless a local user account with the same name as the remote user account is configured on the device before the SSH keys are imported.
- SSH timeout period must be longer than the time of the tac-pac generation time. Otherwise, the VSH log might show %VSHD-2-VSHD_SYSLOG_EOL_ERR error. Ideally, set to 0 (infinity) before collecting tac-pac or showtech.
- Beginning with Cisco NX-OS Release 10.4(3)F, the **show running-config all** command does not display the details of the following commands:
  - no feature telnet
  - no feature nxdb
  - no feature scp-server
  - no feature sftp-server



Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

SNMP synchronization guidelines

- Beginning with Cisco NX-OS Release 10.2(2)F, a new desynchronization CLI is introduced to provide you an option to disable the user synchronization between the SNMP and the security components. For more information, refer to the *Configuring SNMP* chapter in the *System Management Configuration Guide*.

  For more information about the Cisco Nexus 9000 switches that support various features spanning from release 7.0(3)I7(1) to the current release, refer to Nexus Switch Platform Support Matrix.
- When the desynchronization CLI is enabled, remote users will not be synced to SNMP database.

- The security users created using DCNM (also called as Nexus Dashboard Fabric Controller from Release 12.0.1a) will not have a corresponding SNMPv3 profile when the desynchronization CLI is enabled. When the synchronization is disabled, the users created on the security component can log in to the switch, but the switches will not be discovered by the controller, as the controller uses the SNMP configuration created for the security user to discover the switch. Furthermore, the SNMP does not recognize the security users created due to the desynchronized state of the userDB, resulting in failure to discover the switch. Therefore, to have the switches discovered by the controller, the SNMP user must be explicitly created. It is not recommended to use the desynchronization CLI along with DCNM functionality. For more information, refer to the *Cisco Nexus 9000 NX-OS Security Configuration Guide*.

Default settings for SSH and telnet

Use this reference to review the default settings for SSH and telnet.

Table 1: Default SSH and telnet parameters

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Disabled
Telnet port number	23
Maximum number of SSH login attempts	3
SCP server	Disabled
SFTP server	Disabled

Configuring SSH

This section describes how to configure SSH.

Generating SSH server keys

You can generate an SSH server key based on your security requirements. The default SSH server key is an RSA key that is generated using 1024 bits.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no feature ssh**

Example:

```
switch(config)#no feature ssh
```

Disables SSH.

Step 3 **ssh key** {**dsa** [**force**] | **rsa** [*bits*[**force**]] | **ecdsa** [*bits* [**force**]]}

Example:

```
switch(config)#ssh key rsa 2048
```

Generates the SSH server key.

The *bits* argument is the number of bits used to generate the RSA key. The range is from 768 to 2048 . The default value is 1024.

You cannot specify the size of the DSA key. It is always set to 1024 bits.

Use the **force** keyword to replace an existing key.

Note
If you configure ssh key dsa, you must do the following additional configurations: ssh keytypes all and ssh kexalgos all

Step 4 **ssh rekey max-data** *max-data* **max-time** *max-time*i

Example:

```
switch(config)#ssh rekey max-data 1K max-time 1M
```

Configures the rekey parameters.

Step 5 **feature ssh**

Example:

```
switch(config)#feature ssh
```

Enables SSH.

Step 6 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 7 Verify and save the SSH server key configuration.

a) (Optional) **show ssh key** [**dsa** | **rsa** | **ecdsa**] [**md5**]

Example:

```
switch#show ssh key
```

Displays the SSH server keys.

This command displays the fingerprint in SHA256 format by default. SHA256 is more secure than the old default format of MD5. However, the **md5** option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.

b) **show running-config security all**

c) (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Specifying the SSH public keys for user accounts

You can configure an SSH public key to log in using an SSH client without being prompted for a password. You can specify the SSH public key in one of these formats:

- OpenSSH format
- IETF SECSH format

Specify the SSH public keys in IETF SECSH format

You can specify the SSH public keys in IETF SECSH format for user accounts.

Before you begin

Generate an SSH public key in IETF SCHSH format.

Procedure

Step 1 **copy** *server-file* **bootflash:** *filename*

Example:

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
```

Downloads the file containing the SSH key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.

Step 2 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 3 **username** *username* **sshkey file bootflash:** *filename*

Example:

```
switch(config)#username User1 sshkey file bootflash:secsh_file.pub
```

Configures the SSH public key in IETF SECSH format.

Step 4 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 5 (Optional) **show user-account**

Example:

```
switch#show user-account
```

Displays the user account configuration.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Specify the SSH public keys in OpenSSH format

You can specify the SSH public keys in OpenSSH format for user accounts.

Before you begin

Generate an SSH public key in OpenSSH format.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **username** *username* **sshkey** *ssh-key*

Example:

```
switch(config)#username User1 sshkey
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPj
hOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+
XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=
```

Configures the SSH public key in OpenSSH format.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 4 (Optional) **show user-account**

Example:

```
switch#show user-account
```

Displays the user account configuration.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure a maximum number of SSH login attempts

You can configure the maximum number of SSH login attempts. If the user exceeds the maximum number of permitted attempts, the session disconnects.

Note The total number of login attempts includes attempts through public-key authentication, certificate-based authentication, and password-based authentication. If public-key authentication is enabled, it takes priority. If only certificate-based and password-based authentication are enabled, certificate-based authentication takes priority. If you exceed the configured number of login attempts through all of these methods, a message appears indicating that too many authentication failures have occurred.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **ssh login-attempts** *number*

Example:

```
switch(config)#ssh login-attempts 5
```

Configures the maximum number of times that a user can attempt to log into an SSH session. The default maximum number of login attempts is 3. The range is from 1 to 10.

Note

The **no** form of this command removes the previous login attempts value and sets the maximum number of login attempts to the default value of 3.

Step 3 (Optional) **show running-config security all**

Example:

```
switch#show running-config security all
```

Displays the configured maximum number of SSH login attempts.

Step 4 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Starting SSH sessions

You can start SSH sessions using IPv4 or IPv6 to connect to remote devices from the Cisco NX-OS device.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

Procedure

Step 1 **ssh** [*username* **@**]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

Example:

```
switch#ssh 10.10.1.1
```

Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.

Step 2 **ssh6** [*username* **@**]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

Example:

```
switch#ssh6 HostA
```

Creates an SSH IPv6 session to a remote device using IPv6.

Starting SSH sessions from boot mode

You can start SSH sessions from the boot mode of the Cisco NX-OS device to connect to remote devices.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

Procedure

Step 1 **ssh** [*username* **@**]*hostname*

Example:

```
switch(boot)#ssh user1@10.10.1.1
```

Creates an SSH session to a remote device from the boot mode of the Cisco NX-OS device. The default VRF is always used.

Step 2 **exit**

Example:

```
switch(boot)#exit
```

Exits boot mode.

Step 3 **copy scp:**//[*username* **@**]*hostname*/*filepath directory*

Example:

```
switch#copy scp://user1@10.10.1.1/users abc
```

Copies a file from the Cisco NX-OS device to a remote device using the Secure Copy Protocol (SCP). The default VRF is always used.

Configure SSH passwordless file copy

You can copy files from a Cisco NX-OS device to a secure copy (SCP) or secure FTP (SFTP) server without a password. To do so, you must create an RSA or DSA identity that consists of public and private keys for authentication with SSH.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 [**no**] **username** *username* **keypair generate**{**rsa**[*bits* [**force**]] | **dsa** [**force**]}

Example:

```
switch(config)#username user1 keypair generate rsa 2048 force
```

Generates the SSH public and private keys and stores them in the home directory ($HOME/.ssh) of the Cisco NX-OS device for the specified user. The Cisco NX-OS device uses the keys to communicate with the SSH server on the remote machine.

The *bits* argument is the number of bits used to generate the key. The range is from 768 to 2048 . The default value is 1024.

Use the **force** keyword to replace an existing key. The SSH keys are not generated if the **force** keyword is omitted and SSH keys are already present.

Step 3 (Optional) **show username** *username* **keypair**

Example:

```
switch#show username user1 keypair
```

Displays the public key for the specified user.

Note
For security reasons, this command does not show the private key.

Step 4 Required: **username** *username* **keypair export** {**bootflash:** *filename* | **volatile:** *filename*} {**rsa**| **dsa**} [**force**]

Example:

```
switch(config)#username user1 keypair export bootflash:key_rsa rsa
```

Exports the public and private keys from the home directory of the Cisco NX-OS device to the specified bootflash or volatile directory.

Use the **force** keyword to replace an existing key. The SSH keys are not exported if the **force** keyword is omitted and SSH keys are already present.

To export the generated key pair, you are prompted to enter a passphrase that encrypts the private key. The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension. You can now copy this key pair to any Cisco NX-OS device and use SCP or SFTP to copy the public key file (*.pub) to the home directory of the server.

Note
For security reasons, this command can be executed only from global configuration mode.

Step 5 Required: **username** *username* **keypair import** {**bootflash:** *filename* | **volatile:** *filename*} {**rsa**| **dsa**} [**force**]

Example:

```
switch(config)#username user1 keypair import bootflash:key_rsa rsa
```

Imports the exported public and private keys from the specified bootflash or volatile directory to the home directory of the Cisco NX-OS device.

Use the **force** keyword to replace an existing key. The SSH keys are not imported if the **force** keyword is omitted and SSH keys are already present.

To import the generated key pair, you are prompted to enter a passphrase that decrypts the private key. The private key is imported as the file that you specify, and the public key is imported with the same filename followed by a .pub extension.

Note
For security reasons, this command can be executed only from global configuration mode.

Note

Only the users whose keys are configured on the server are able to access the server without a password.

What to do next

On the SCP or SFTP server, use the following command to append the public key stored in the *.pub file (for example, key_rsa.pub) to the authorized_keys file:

$ cat key_rsa.pub>> $HOME/.ssh/ authorized_keys

You can now copy files from the Cisco NX-OS device to the server without a password using standard SSH and SCP commands.

Configure SCP and SFTP servers

You can configure an SCP or SFTP server on the Cisco NX-OS device in order to copy files to and from a remote device. After you enable the SCP or SFTP server, you can execute an SCP or SFTP command on the remote device to copy the files to or from the Cisco NX-OS device.

Note The arcfour and blowfish cipher options are not supported for the SCP server.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 [**no**] **feature scp-server**

Example:

```
switch(config)#feature scp-server
```

Enables or disables the SCP server on the Cisco NX-OS device.

Step 3 Required: [**no**] **feature sftp-server**

Example:

```
switch(config)#feature sftp-server
```

Enables or disables the SFTP server on the Cisco NX-OS device.

Step 4 Required: **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 5 (Optional) **show running-config security**

Example:

```
switch#show running-config security
```

Displays the configuration status of the SCP and SFTP servers.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configure x.509v3 Certificate-Based SSH authentication

You can configure SSH authentication using X.509v3 certificates.

Before you begin

Enable the SSH server on the remote device.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **username** *user-id* [**password** [**0** | **5**] *password*]

Example:

```
switch(config)#username jsmith password 4Ty18Rnt
```

Configures a user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters for both local and remote users. Valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hyphen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames.

Usernames must begin with an alphanumeric character.

The default password is undefined. The **0** option indicates that the password is clear text, and the **5** option indicates that the password is encrypted. The default is **0** (clear text).

Note
If you do not specify a password, the user might not be able to log in to the Cisco NX-OS device.

Note

If you create a user account with the encrypted password option, the corresponding SNMP user will not be created.

Note
When the desynchronization CLI is enabled, if you create a user account, the corresponding SNMP user will not be created.

Step 3 **username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**}

Example:

```
switch(config)#username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
rsa
```

Specifies an SSH X.509 certificate distinguished name and DSA or RSA algorithm to use for authentication for an existing user account. The distinguished name can be up to 512 characters and must follow the format shown in the examples. Make sure the email address and state are configured as emailAddress and ST, respectively.

Step 4 [**no**] **crypto ca trustpoint** *trustpoint*

Example:

```
switch(config)#crypto ca trustpoint winca
switch(config-trustpoint)#
```

Configures a trustpoint.

Note
Before you delete a trustpoint using the **no** form of this command, you must first delete the CRL and CA certificate, using the **delete crl** and **delete ca-certificate** commands.

Step 5 **crypto ca authenticate** *trustpoint*

Example:

```
switch(config-trustpoint)#crypto ca authenticate winca
```

Configures a CA certificate for the trustpoint.

Note
To delete a CA certificate, enter the **delete ca-certificate** command in the trustpoint configuration mode.

Step 6 (Optional) **crypto ca crl request** *trustpoint* **bootflash:** *static-crl* **.crl**

Example:

```
switch(config-trustpoint)#crypto ca crl request winca bootflash:crllist.crl
```

This command is optional but highly recommended. Configures the certificate revocation list (CRL) for the trustpoint. The CRL file is a snapshot of the list of revoked certificates by the trustpoint. This static CRL list is manually copied to the device from the Certification Authority (CA).

Note
Static CRL is the only supported revocation check method.

Note
To delete the CRL, enter the **delete crl** command.

Step 7 Verify and save the configuration.

a) (Optional) **show crypto ca certificates**

Example:

```
switch#show crypto ca certificates
```

Displays the configured certificate chain and associated trustpoint.

b) (Optional) **show crypto ca crl** *trustpoint*

Example:

```
switch#show crypto ca crl winca
```

Displays the contents of the CRL list of the specified trustpoint.

c) (Optional) **show user-account**

Example:

```
switch#show user-account
```

Displays configured user account details.

d) (Optional) **show users**

Example:

```
switch#show users
```

Displays the users logged into the device.

e) (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Configuring SSH-Cert-Authorization on TACACS servers

Beginning with Cisco NX-OS Release 10.4(3)F, the Cisco Nexus 9000 Series switches support SSH authorization using X.509 certificates through a TACACS+ server. This feature is not supported with RADIUS. This feature can be enabled using

aaa authorization ssh-certificate default group *tac-group-name* command. For more information on configuration, see
Configure AAA SSH-Cert-Authorization on TACACS servers.

Configure legacy SSH algorithm SupportCustomizing SSH cryptographic algorithms

Cisco Nexus 9000 switches support strong algorithms by default. You can choose to remain with the default mode that enables only strong algorithms as defined by Cisco Product Security Baseline (PSB) or allow all supported algorithms. Note that these algorithms are applicable to the incoming server connections. You can also configure support for SSH key exchange algorithms, message authentication codes (MACs), key types, and ciphers.

Note MAC algorithms are negotiated and enforced only for non-AEAD ciphers (such as aes256-ctr, aes128-cbc), whereas AEAD ciphers (such as aes128-gcm@openssh.com, aes256-gcm@openssh.com, or chacha20-poly1305@openssh.com) provide built-in integrity protection that renders any client-specified MAC unused, in accordance with RFC 5647 standard SSH protocol behavior.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
```

Enters the global configuration mode.

Step 2 (Optional) **ssh kexalgos**[**all** | **key-exchangealgorithm-name**]

Example:

```
switch(config)#ssh kexalgos ecdhsha2-nistp384
```

Use the **all** keyword to enable all supported KexAlgorithms which are the key exchange methods that are used to generate per-connection keys.

Note
All KexAlgorithms are enabled by default, but if you need to customize your configuration, you can specify the required algorithms and apply permit or deny rules to align with your specific security requirements.

To enable only the **ecdh-sha2-nistp384** KexAlgorithm, use the **ecdh-sha2-nistp384** keyword.

Note
Starting with Cisco NX-OS Release 10.4(2)F, you can configure any of the supported KexAlgorithms. From this release, keyword **ecdh-sha2-nistp384** is deprecated.

Supported KexAlgorithms are:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- ecdh-sha2-nistp256
- ecdh-sha2-nistp521

Unsupported KexAlgorithms are:

- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha256

Step 3 (Optional) **ssh macs [all | mac-name]**

Example:

```
switch(config)#ssh macs hmacsha2-256-etm@openssh.com
```

Enables all supported MACs which are the message authentication codes used to detect traffic modification.

Supported MACs are:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha1-etm@openssh.com

Note
Starting with Cisco NX-OS Release 10.4(2)F, you can configure any of the supported MACs.

Step 4 (Optional) **ssh ciphers**[**all** | **cipher-name**]

Example:

```
switch(config)#ssh ciphers aes192-ctr
```

Use the **all** keyword to enable all supported ciphers to encrypt the connection.

Supported ciphers are:

- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- chacha20-poly1305@openssh.com

Note
Starting with Cisco NX-OS Release 10.4(2)F, you can configure any of the supported ciphers. From this release, keyword **aes256-gcm** is deprecated.

Step 5 (Optional) **ssh keytypes [all | keytype-string]**

Example:

```
switch(config)#ssh keytypes ecdsa-sha2-nistp256
```

Enables all supported PubkeyAcceptedKeyTypes which are the public key algorithms that the server can use to authenticate itself to the client.

Supported key types are:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-dss
- rsa-sha2-256
- ssh-rsa-cert-v01@openssh.com

Configure legacy SSH algorithm SupportCustomizing SSH cryptographic algorithms continued

- ssh-rsa

Note
Starting with Cisco NX-OS Release 10.4(2)F, you can configure any of the supported keytypes.

Note
To enable rsa, dsa, and ecdsa key types, you need to generate corresponding SSH host keys.

Example configuration:

```
switch(config)#ssh key rsa 2048
switch(config)#ssh key dsa
switch(config)#ssh key ecdsa 256
```

Users can check the supported algorithms using **show ssh [ciphers | macs | keytypes | kexalogs | version]** commands.

```
switch# show ssh ciphers
Cipher                                          Status    FIPS
-----------------------------------------------------------------
aes128-ctr                                   permitted     yes
aes192-ctr                                      denied     yes
aes256-ctr                                   permitted     yes
aes128-cbc                                      denied     yes
aes192-cbc                                      denied     yes
aes256-cbc                                      denied     yes
aes256-gcm@openssh.com                    permitted     yes
aes128-gcm@openssh.com                     permitted     yes
chacha20-poly1305@openssh.com              permitted      no

switch# show ssh mac
MAC                                             Status    FIPS
-----------------------------------------------------------------
hmac-sha2-256-etm@openssh.com              permitted      no
```

```
hmac-sha2-512-etm@openssh.com              permitted      no
hmac-sha1-etm@openssh.com                  permitted      no
hmac-sha2-256                              permitted     yes
hmac-sha2-512                              permitted     yes
hmac-sha1                                  permitted     yes
hmac-sha1-96                             unsupported      no
hmac-md5                                 unsupported      no
hmac-md5-96                              unsupported      no
umac-64@openssh.com                      unsupported      no
umac-128@openssh.com                     unsupported      no
hmac-sha1-96-etm@openssh.com             unsupported      no
hmac-md5-etm@openssh.com                 unsupported      no
umac-64-etm@openssh.com                  unsupported      no
umac-128-etm@openssh.com                 unsupported      no


switch# show ssh keytypes
Keytype                                          Status    FIPS
-------------------------------------------------------------
ecdsa-sha2-nistp256-cert-v01@openssh.com   permitted      no
          <<Currently not suppported>>
ecdsa-sha2-nistp384-cert-v01@openssh.com   permitted      no
          <<Currently not suppported>>
ecdsa-sha2-nistp521-cert-v01@openssh.com   permitted      no
          <<Currently not suppported>>
ssh-rsa-cert-v01@openssh.com               permitted      no
ecdsa-sha2-nistp256                        permitted     yes
ecdsa-sha2-nistp384                        permitted     yes
ecdsa-sha2-nistp521                        permitted      no
rsa-sha2-256                               permitted      no
ssh-rsa                                    permitted     yes
ssh-dss                                       denied      no
ssh-ed25519                              unsupported      no
ssh-ed25519-cert-v01@openssh.com         unsupported      no
ssh-dss-cert-v01@openssh.com             unsupported      no


switch# show ssh kexalgos
KexAlgorithm                                     Status    FIPS
-------------------------------------------------------------
curve25519-sha256                          permitted      no
curve25519-sha256@libssh.org               permitted      no
ecdh-sha2-nistp256                         permitted     yes
ecdh-sha2-nistp384                         permitted     yes
ecdh-sha2-nistp521                         permitted     yes
diffie-hellman-group16-sha512              permitted     yes
diffie-hellman-group14-sha1                permitted     yes
diffie-hellman-group14-sha256              permitted      no


switch# show ssh version
CiscoSSH 1.9.29, OpenSSH_8.3p1, CiscoSSL 1.1.1t.7.2.500
```

Algorithms supported - FIPS mode enabled

The list of algorithms supported when the FIPs mode is enabled are as follows:

Table 2: Algorithms supported - FIPS mode enabled

Algorithms	Supported	Unsupported	
ciphers	• aes128-ctr • aes256-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com • chacha20-poly1305@openssh.com	• aes192-ctr • aes128-cbc • aes192-cbc • aes256-cbc	
hmac	• hmac-sha2-256 • hmac-sha2-512 • hmac-sha1 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-sha1-etm@openssh.com	-	
kexalgo	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group16-sha512 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • curve25519-sha256@libssh.org • curve25519-sha256	-	
	keytypes	• ecdsa-sha2-nistp256-cert-v01@openssh.com • ecdsa-sha2-nistp384-cert-v01@openssh.com • ecdsa-sha2-nistp521-cert-v01@openssh.com • ssh-rsa-cert-v01@openssh.com • rsa-sha2-256 • ssh-rsa • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521	• ed

Change the default SSH server port

Beginning with Cisco NX-OS Cisco Release 9.2(1), you can change the SSHv2 port number from the default port number 22. Encryptions used while changing the default SSH port provides you with connections that support stronger privacy and session integrity

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no feature ssh**

Example:

```
switch(config)#no feature ssh
```

Disables SSH.

Step 3 **show sockets** *local-port-range*

Example:

```
switch#show sockets local-port-range
Kstack local port range (15001 - 22002)
Netstack local port range (22003 - 65535)
```

Displays the available port range.

Step 4 **ssh port** *local-port*

Example:

```
switch(config)#ssh port 58003
```

Configures the port.

Note
When you upgrade from an earlier release to Release 9.3(1) or later releases, ensure that features with user-defined SSH port, are within the following range:

- For Release 9.3(1) and Release 9.3(2): Kstack local port range is from 15001 to 58000, netstack local port range is from 58001 - 63535, and nat port range is from 63536 to 65535
- From Release 9.3(3): Kstack local port range is from 15001 to 58000, netstack local port range is from 58001 to 60535, and nat port range is from 60536 to 65535

Step 5 **feature ssh**

Example:

```
switch(config)#feature ssh
```

Enables SSH.

Step 6 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 7 (Optional) **show running-config security all**

Example:

```
switch#show running-config security all
```

Displays the security configuration.

Step 8 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Clear SSH hosts

When you download a file from a server using SCP or SFTP, or when you start an SSH session from this device to a remote host, you establish a trusted SSH relationship with that server. You can clear the list of trusted SSH servers for your user account.

Procedure

clear ssh hosts

Example:

```
switch#clear ssh hosts
```

Clears the SSH host sessions and the known host file.

Disable the SSH server

By default, the SSH server is enabled on the Cisco NX-OS device. You can disable the SSH server to prevent SSH access to the switch.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no feature ssh**

Example:

```
switch(config)#no feature ssh
```

Disables SSH.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 4 (Optional) **show ssh server**

Example:

```
switch#show ssh server
```

Displays the SSH server configuration.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Delete SSH server keys

You can delete SSH server keys on the Cisco NX-OS device after you disable the SSH server.

Note To reenable SSH, you must first generate an SSH server key.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **no feature ssh**

Example:

```
switch(config)#no feature ssh
```

Disables SSH.

Step 3 **no ssh key** [**dsa** | **rsa** | **ecdsa**]

Example:

```
switch(config)#no ssh key rsa
```

Deletes the SSH server key.

The default is to delete all the SSH keys.

Step 4 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 5 (Optional) **show ssh key**

Example:

```
switch#show ssh key
```

Displays the SSH server key configuration.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Related Topics

Generating SSH server keys, on page 5

Clear SSH sessions

You can clear SSH sessions from the Cisco NX-OS device.

Procedure

Step 1 **show users**

Example:

```
switch#show users
```

Displays user session information.

Step 2 **clear line** *vty-line*

Example:

```
switch#clear line pts/12
```

Clears a user SSH session.

Configuring telnet

This section describes how to configure Telnet on the Cisco NX-OS device.

Enable the telnet server

You can enable the Telnet server on the Cisco NX-OS device. By default, the Telnet server is disabled.

Procedure

Step 1 **configure terminal**

Example:

```
switch#configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **feature telnet**

Example:

```
switch(config)#feature telnet
```

Enables the Telnet server. The default is disabled.

Step 3 **exit**

Example:

```
switch(config)#exit
switch#
```

Exits global configuration mode.

Step 4 (Optional) **show telnet server**

Example:

```
switch#show telnet server
```

Displays the Telnet server configuration.

Step 5 (Optional) **copy running-config startup-config**

Example:

```
switch#copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Starting telnet sessions to remote devices

You can start Telnet sessions to connect to remote devices from the Cisco NX-OS device. You can start Telnet sessions using either IPv4 or IPv6.

Before you begin

Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.

Enable the Telnet server on the Cisco NX-OS device.

Enable the Telnet server on the remote device.

Procedure

Step 1 **telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]

Example:

```
switch#telnet 10.10.1.1
```

Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.

Step 2 **telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]

Example:

```
switch#telnet6 2001:0DB8::ABCD:1 vrf management
```

Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.

Related Topics

Enable the telnet server, on page 26

Clear telnet sessions

You can clear Telnet sessions from the Cisco NX-OS device.

Before you begin

Enable the Telnet server on the Cisco NX-OS device.

Procedure

Step 1 **show users**

Example:

```
switch#show users
```

Displays user session information.

Step 2 **clear line** *vty-line*

Example:

```
switch#clear line pts/12
```

Clears a user Telnet session.

SSH and telnet configuration verification commands

Use this reference to verify the SSH and telnet configuration.

Configuration information configuration example

To display the SSH and Telnet configuration information, perform one of the following tasks:

SSH and telnet configuration verification commands

Table 3: SSH and telnet configuration verification commands

Command	Purpose
show ssh key [**dsa** | **rsa**] [**md5**]	Displays the SSH server keys. For Cisco NX-OS Release 7.0(3)I4(6) and 7.0(3)I6(1) and any later releases, this command displays the fingerprint in SHA256 format by default. SHA256 is more secure than the old default format of MD5. However, the **md5** option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.
show running-config security [**all**]	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.
show telnet server	Displays the Telnet server configuration.
show username *username* **keypair**	Displays the public key for the specified user.
show user-account	Displays configured user account details.
show users	Displays the users logged into the device.
show crypto ca certificates	Displays the configured CA certificate and associated trustpoint for X.509v3 certificate-based SSH authentication.
show crypto ca crl *trustpoint*	Displays the contents of the CRL list of the specified trustpoint for X.509v3 certificate-based SSH authentication.

Configuration example for SSH

The following example shows how to configure SSH with an OpenSSH key:

Procedure

Step 1 Disable the SSH server.

Example:

```
switch#configure terminal
switch(config)#no feature ssh
```

Step 2 Generate an SSH server key.

Example:

```
switch(config)#ssh key rsa
generating rsa key(1024 bits)......
generated rsa key
```

Step 3 Enable the SSH server.

Example:

```
switch(config)#feature ssh
```

Step 4 Display the SSH server key.

Example:

```
switch#show ssh key
could not retrieve dsa key information
**************************************
rsa Keys generated:Tue Mar 14 13:13:47 2017

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDh4+DZboQJbJt10nJhgKBYL5lOlhsFM2oZRi9+JqEU
GA44I9ej+E5NIRZ1x8ohIt6Vx9Et5csO7Pw72rjUwR3UPmuAm79k7I/SyLGEP3WUL7sqbLvNF5GqKXph
oqMT075WUdbGWphorA2g0tTObRrFIQBJVQ0SSBh3oEaaALqYUQ==

bitcount:1024
fingerprint:
SHA256:V6KAeLAiKRRUPBZm1Yq3rl6JW7Eo7vhLi6CXYxnD/+Y
**************************************
**************************************


switch#show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2013

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr
+MZm99n2U0ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39
HmXL6VgpRVn1XQFiBwn4na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
00:00:5E:00:53:01:00:00:5E:00:53:02:15:5d:9a:df
**************************************
could not retrieve dsa key information
**************************************
```

Step 5 Specify the SSH public key in OpenSSH format.

Example:

```
switch(config)#username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tplx8=
```

Step 6 Save the configuration.

Example:

```
switch#copy running-config startup-config
```

Configuration example for SSH passwordless file copy

The following example shows how to copy files from a Cisco NX-OS device to a secure copy (SCP) or secure FTP (SFTP) server without a password:

Procedure

Step 1 Generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the specified user.

Example:

```
switch#configure terminal
switch(config)#username admin keypair generate rsa
generating rsa key(1024 bits)......
generated rsa key
```

Step 2 Display the public key for the specified user.

Example:

```
switch#show username admin keypair
**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
00:00:5E:00:53:01:00:00:5E:00:53:02:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
```

Step 3 Export the public and private keys from the home directory of the Cisco NX-OS device to the specified bootflash directory.

Example:

```
switch(config)#username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
        951     Jul 09 11:13:59 2013  key_rsa
        221     Jul 09 11:14:00 2013  key_rsa.pub
.
.
```

Step 4 After copying these two files to another Cisco NX-OS device using the **copy scp** or **copy sftp** command, import them to the home directory of the Cisco NX-OS device.

Example:

```
switch(config)#username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch#show username admin keypair
**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
00:00:5E:00:53:01:00:00:5E:00:53:02:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
switch(config)#
```

Step 5 On the SCP or SFTP server, append the public key stored in key_rsa.pub to the authorized_keys file.

Example:

```
$ cat key_rsa.pub>> $HOME/.ssh/ authorized_keys
```

You can now copy files from the Cisco NX-OS device to the server without a password using standard SSH and SCP commands.

Step 6 (Optional) Repeat this procedure for the DSA keys.

Configuration example for x.509v3 Certificate-Based SSH authentication

The following example shows how to configure SSH authentication using X.509v3 certificates:

Configuration example for x.509v3 Certificate-Based SSH authentication information

Note Beginning with Cisco NX-OS Release 10.4(3)F, the Cisco Nexus 9000 Series switches support SSH authorization using X.509 certificates through a TACACS+ server. This feature is not supported with RADIUS.

Configuration example for x.509v3 Certificate-Based SSH authentication information command examples

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
rsa
crypto ca trustpoint tp1
crypto ca authenticate tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=00:00:5E:00:53:01:00:00:5E:00:53:02:00:00:5E:00:53:03:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /CN=SecDevCA
    Last Update: Aug 8 20:03:15 2016 GMT
    Next Update: Aug 16 08:23:15 2016 GMT
    CRL extensions:
        X509v3 Authority Key Identifier:
            keyid:00:00:5E:00:53:04:00:00:5E:00:53:05:00:00:5E:00:53:06:FF:2A

show user-account
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN =
user1; Algo: x509v3-sign-rsa

show users
NAME      LINE        TIME          IDLE      PID         COMMENT
user1     pts/1       Jul 27 18:43  00:03     18796      (10.10.10.1)   session=ssh
```

Additional references for SSH and telnet

Use this reference to find additional references for SSH and telnet.

This section describes additional information related to implementing SSH and Telnet.

Related Documents

Table 4: Related documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
VRF configuration	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*

RFCs

Table 5: Rfcs

RFCs	Title
RFC 6187	*X.509v3 Certificates for Secure Shell Authentication*

MIBs

Table 6: MIBs

MIBs	MIBs Link
MIBs related to SSH and Telnet	To locate and download supported MIBs, go to the following URL: https://example.com/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html