



# 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 4](#)
- [Configuring SSH , on page 5](#)
- [Configuring Telnet, on page 21](#)
- [Verifying the SSH and Telnet Configuration, on page 23](#)
- [Configuration Example for SSH, on page 24](#)
- [Configuration Example for SSH Passwordless File Copy, on page 25](#)
- [Configuration Example for X.509v3 Certificate-Based SSH Authentication, on page 27](#)
- [Additional References for SSH and Telnet, on page 27](#)

## 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 Algorithm (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.

## 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

SSH and Telnet have the following configuration guidelines and limitations:

- The Cisco NX-OS software supports only SSH version 2 (SSHv2).
- Cisco NX-OS does not support remote TACACS authentication.
- 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 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.



**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.

- 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

This table lists the default settings for SSH and Telnet parameters.

**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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no feature ssh</b> <b>Example:</b> <pre>switch(config)# no feature ssh</pre>	Disables SSH.
<b>Step 3</b>	<b>ssh key {dsa [force]   rsa [bits[force]]   ecdsa [bits [force]]}</b> <b>Example:</b> <pre>switch(config)# ssh key rsa 2048</pre>	<p>Generates the SSH server key.</p> <p>The <i>bits</i> argument is the number of bits used to generate the RSA key. The range is from 768 to 2048. The default value is 1024.</p> <p>You cannot specify the size of the DSA key. It is always set to 1024 bits.</p> <p>Use the <b>force</b> keyword to replace an existing key.</p> <p><b>Note</b> If you configure <code>ssh key dsa</code>, you must do the following additional configurations: <code>ssh keytypes all</code> and <code>ssh kexalgs all</code></p>
<b>Step 4</b>	<b>ssh rekey max-data max-data max-time max-time</b> <b>Example:</b> <pre>switch(config)# ssh rekey max-data 1K max-time 1M</pre>	Configures the rekey parameters.
<b>Step 5</b>	<b>feature ssh</b> <b>Example:</b> <pre>switch(config)# feature ssh</pre>	Enables SSH.

	Command or Action	Purpose
<b>Step 6</b>	<b>exit</b>  <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.
<b>Step 7</b>	(Optional) <b>show ssh key [dsa   rsa   ecdsa] [md5 ]</b>  <b>Example:</b> 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 <b>md5</b> option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.
<b>Step 8</b>	<b>show run security all</b>	
<b>Step 9</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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

### Specifying 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

	Command or Action	Purpose
<b>Step 1</b>	<b>copy <i>server-file</i> bootflash:<i>filename</i></b>  <b>Example:</b> 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.

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 3</b>	<b>username <i>username</i> sshkey file</b> <b>bootflash:<i>filename</i></b> <b>Example:</b> switch(config)# username User1 sshkey file bootflash:secsh_file.pub	Configures the SSH public key in IETF SECSH format.
<b>Step 4</b>	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.
<b>Step 5</b>	(Optional) <b>show user-account</b> <b>Example:</b> switch# show user-account	Displays the user account configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Specifying 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>username <i>username</i> sshkey <i>ssh-key</i></b> <b>Example:</b> switch(config)# username User1 sshkey ssh-rsa AAAEBnaClyc2FAWELAAIA719-F6QZ19G3FDxwK0iVH7YUuA50r7gEP h0BmsigZKilnIf/Dnm+LNp/4ow7to+MRFY/GHLNIG6gig30c66+	Configures the SSH public key in OpenSSH format.

	Command or Action	Purpose
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>show user-account</b>  <b>Example:</b> <pre>switch# show user-account</pre>	Displays the user account configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Configuring 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>ssh login-attempts <i>number</i></b>  <b>Example:</b> <pre>switch(config)# ssh login-attempts 5</pre>	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.



	Command or Action	Purpose
		<b>Note</b> The <b>no</b> form of this command removes the previous login attempts value and sets the maximum number of login attempts to the default value of 3.
<b>Step 3</b>	(Optional) <b>show running-config security all</b>  <b>Example:</b> switch(config)# show running-config security all	Displays the configured maximum number of SSH login attempts.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) 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

	Command or Action	Purpose
<b>Step 1</b>	<b>ssh</b> [ <i>username@</i> ]{ <i>ipv4-address</i>   <i>hostname</i> } [ <i>vrf vrf-name</i> ]  <b>Example:</b> switch# ssh 10.10.1.1	Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.
<b>Step 2</b>	<b>ssh6</b> [ <i>username@</i> ]{ <i>ipv6-address</i>   <i>hostname</i> } [ <i>vrf vrf-name</i> ]  <b>Example:</b> 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

	Command or Action	Purpose
<b>Step 1</b>	<b>ssh</b> <i>[username@]hostname</i> <b>Example:</b> 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.
<b>Step 2</b>	<b>exit</b> <b>Example:</b> switch(boot) # exit	Exits boot mode.
<b>Step 3</b>	<b>copy scp</b> :// <i>[username@]hostname/filepath directory</i> <b>Example:</b> 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.

## Configuring 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] username <i>username</i> keypair generate {rsa [<i>bits</i> <b>force</b>]   dsa [<b>force</b>]}</b> <b>Example:</b> switch(config)# username user1 keypair generate rsa 2048 force	<p>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.</p> <p>The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 2048. The default value is 1024.</p> <p>Use the <b>force</b> keyword to replace an existing key. The SSH keys are not generated if the <b>force</b> keyword is omitted and SSH keys are already present.</p>

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show username</b> <i>username</i> <b>keypair</b> <b>Example:</b> <pre>switch(config)# show username user1 keypair</pre>	Displays the public key for the specified user. <b>Note</b> For security reasons, this command does not show the private key.
<b>Step 4</b>	Required: <b>username</b> <i>username</i> <b>keypair export</b> { <b>bootflash:filename</b>   <b>volatile:filename</b> } { <b>rsa</b>   <b>dsa</b> } [ <b>force</b> ] <b>Example:</b> <pre>switch(config)# username user1 keypair export bootflash:key_rsa rsa</pre>	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 <b>force</b> keyword to replace an existing key. The SSH keys are not exported if the <b>force</b> 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. <b>Note</b> For security reasons, this command can be executed only from global configuration mode.
<b>Step 5</b>	Required: <b>username</b> <i>username</i> <b>keypair import</b> { <b>bootflash:filename</b>   <b>volatile:filename</b> } { <b>rsa</b>   <b>dsa</b> } [ <b>force</b> ] <b>Example:</b> <pre>switch(config)# username user1 keypair import bootflash:key_rsa rsa</pre>	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 <b>force</b> keyword to replace an existing key. The SSH keys are not imported if the <b>force</b> 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. <b>Note</b> For security reasons, this command can be executed only from global configuration mode.

	Command or Action	Purpose
		<b>Note</b> 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.

## Configuring 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**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature scp-server</b>  <b>Example:</b> switch(config)# feature scp-server	Enables or disables the SCP server on the Cisco NX-OS device.
<b>Step 3</b>	Required: <b>[no] feature sftp-server</b>  <b>Example:</b> switch(config)# feature sftp-server	Enables or disables the SFTP server on the Cisco NX-OS device.
<b>Step 4</b>	Required: <b>exit</b>  <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) <b>show running-config security</b> <b>Example:</b> switch# show running-config security	Displays the configuration status of the SCP and SFTP servers.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring X.509v3 Certificate-Based SSH Authentication

You can configure SSH authentication using X.509v3 certificates. Cisco NX-OS does not support remote TACACS authentication.

### Before you begin

Enable the SSH server on the remote device.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>username <i>user-id</i> [password [0 5] <i>password</i>]</b> <b>Example:</b> switch(config)# username jsmith password 4Ty18Rnt	<p>Configures a user account. The <i>user-id</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. 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.</p> <p>Usernames must begin with an alphanumeric character.</p> <p>The default password is undefined. The <b>0</b> option indicates that the password is clear text, and the <b>5</b> option indicates that the password is encrypted. The default is <b>0</b> (clear text).</p> <p><b>Note</b> If you do not specify a password, the user might not be able to log in to the Cisco NX-OS device.</p>

	Command or Action	Purpose
		<p><b>Note</b> If you create a user account with the encrypted password option, the corresponding SNMP user will not be created.</p> <p><b>Note</b> When the desynchronization CLI is enabled, if you create a user account, the corresponding SNMP user will not be created.</p>
<b>Step 3</b>	<p><code>username <i>user-id</i> ssh-cert-dn <i>dn-name</i> {<i>dsa</i>   <i>rsa</i>}</code></p> <p><b>Example:</b></p> <pre>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</pre>	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 <code>emailAddress</code> and <code>ST</code> , respectively.
<b>Step 4</b>	<p><code>[no] crypto ca trustpoint <i>trustpoint</i></code></p> <p><b>Example:</b></p> <pre>switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</pre>	<p>Configures a trustpoint.</p> <p><b>Note</b> Before you delete a trustpoint using the <b>no</b> form of this command, you must first delete the CRL and CA certificate, using the <b>delete crl</b> and <b>delete ca-certificate</b> commands.</p>
<b>Step 5</b>	<p><code>crypto ca authenticate <i>trustpoint</i></code></p> <p><b>Example:</b></p> <pre>switch(config-trustpoint)# crypto ca authenticate winca</pre>	<p>Configures a CA certificate for the trustpoint.</p> <p><b>Note</b> To delete a CA certificate, enter the <b>delete ca-certificate</b> command in the trustpoint configuration mode.</p>
<b>Step 6</b>	<p>(Optional) <code>crypto ca crl request <i>trustpoint</i> bootflash:<i>static-crl.crl</i></code></p> <p><b>Example:</b></p> <pre>switch(config-trustpoint)# crypto ca crl request winca bootflash:crllist.crl</pre>	<p>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).</p> <p><b>Note</b> Static CRL is the only supported revocation check method.</p> <p><b>Note</b> To delete the CRL, enter the <b>delete crl</b> command.</p>

	Command or Action	Purpose
<b>Step 7</b>	(Optional) <b>show crypto ca certificates</b> <b>Example:</b> switch(config-trustpoint)# show crypto ca certificates	Displays the configured certificate chain and associated trustpoint.
<b>Step 8</b>	(Optional) <b>show crypto ca crl trustpoint</b> <b>Example:</b> switch(config-trustpoint)# show crypto ca crl winca	Displays the contents of the CRL list of the specified trustpoint.
<b>Step 9</b>	(Optional) <b>show user-account</b> <b>Example:</b> switch(config-trustpoint)# show user-account	Displays configured user account details.
<b>Step 10</b>	(Optional) <b>show users</b> <b>Example:</b> switch(config-trustpoint)# show users	Displays the users logged into the device.
<b>Step 11</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-trustpoint)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Configuring Legacy SSH Algorithm Support

You can configure support for legacy SSH security algorithms, message authentication codes (MACs), key types, and ciphers.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal	Enters the global configuration mode.
<b>Step 2</b>	(Optional) <b>ssh kexalgs [all]</b> <b>Example:</b> switch(config)# ssh kexalgs all	Use the <b>all</b> keyword to enable all supported KexAlgorithms which are the key exchange methods that are used to generate per-connection keys.  Supported KexAlgorithms are: <ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• diffie-hellman-group-exchange-sha256</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• diffie-hellman-group1-sha1</li> </ul> <p><b>Note</b> This algorithm isn't supported from Cisco NX-OS Release 9.3(5). Upgrade your SSH client.</p> <ul style="list-style-type: none"> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group1-sha1</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> </ul>
<b>Step 3</b>	(Optional) <code>ssh macs all</code> <b>Example:</b> <pre>switch(config)# ssh macs all</pre>	Enables all supported MACs which are the message authentication codes used to detect traffic modification. Supported MACs are: <ul style="list-style-type: none"> <li>• hmac-sha1</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> </ul>
<b>Step 4</b>	(Optional) <code>ssh ciphers [ all ]</code> <b>Example:</b> <pre>switch(config)# ssh ciphers all</pre>	Use the <b>all</b> keyword to enable all supported ciphers to encrypt the connection. Supported ciphers are: <ul style="list-style-type: none"> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>
<b>Step 5</b>	(Optional) <code>ssh keytypes all</code> <b>Example:</b> <pre>switch(config)# ssh keytypes all</pre>	Enables all supported <code>PubkeyAcceptedKeyTypes</code> which are the public key algorithms that the server can use to authenticate itself to the client. Supported key types are:



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• ssh-dss</li> <li>• ssh-rsa</li> </ul>

## 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	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> </ul>
hmac	<ul style="list-style-type: none"> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• hmac-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha1-etm@openssh.com</li> </ul>
kexalgo	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group14-sha256</li> </ul>	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• curve25519-sha256@libssh.org</li> </ul>
keytypes	<ul style="list-style-type: none"> <li>• rsa-sha2-256</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> </ul>	ssh-rsa

## Changing 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no feature ssh</b>  <b>Example:</b> <pre>switch(config)# no feature ssh</pre>	Disables SSH.
<b>Step 3</b>	<b>show sockets local-port-range</b>  <b>Example:</b> <pre>switch(config)# show sockets local port range (15001 - 58000) switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535)  switch# show sockets local-port-range Kstack local port range (15001 - 22002) Netstack local port range (22003 - 65535)</pre>	Displays the available port range.
<b>Step 4</b>	<b>ssh port local-port</b>  <b>Example:</b> <pre>switch(config)# ssh port 58003</pre>	Configures the port.  <b>Note</b> 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: <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> </ul>

	Command or Action	Purpose
<b>Step 5</b>	<b>feature ssh</b> <b>Example:</b> switch(config)# feature ssh	Enables SSH.
<b>Step 6</b>	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.
<b>Step 7</b>	(Optional) <b>show running-config security all</b> <b>Example:</b> switch# ssh port 58003	Displays the security configuration.
<b>Step 8</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Clearing 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

	Command or Action	Purpose
<b>Step 1</b>	<b>clear ssh hosts</b> <b>Example:</b> switch# clear ssh hosts	Clears the SSH host sessions and the known host file.

## Disabling 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	Disables SSH.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>show ssh server</b> <b>Example:</b> switch# show ssh server	Displays the SSH server configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

## Deleting 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

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	Disables SSH.
<b>Step 3</b>	<b>no ssh key [dsa   rsa   ecdsa]</b> <b>Example:</b> switch(config)# no ssh key rsa	Deletes the SSH server key. The default is to delete all the SSH keys.
<b>Step 4</b>	<b>exit</b> <b>Example:</b>	Exits global configuration mode.

	Command or Action	Purpose
	switch(config)# exit switch#	
<b>Step 5</b>	(Optional) <b>show ssh key</b>  <b>Example:</b> switch# show ssh key	Displays the SSH server key configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

**Related Topics**

[Generating SSH Server Keys](#), on page 5

## Clearing SSH Sessions

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>show users</b>  <b>Example:</b> switch# show users	Displays user session information.
<b>Step 2</b>	<b>clear line vty-line</b>  <b>Example:</b> switch(config)# clear line pts/12	Clears a user SSH session.

## Configuring Telnet

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

### Enabling the Telnet Server

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
<b>Step 2</b>	<b>feature telnet</b>  <b>Example:</b> switch(config)# feature telnet	Enables the Telnet server. The default is disabled.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> switch(config)# exit switch#	Exits global configuration mode.
<b>Step 4</b>	(Optional) <b>show telnet server</b>  <b>Example:</b> switch# show telnet server	Displays the Telnet server configuration.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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

	Command or Action	Purpose
<b>Step 1</b>	<b>telnet</b> { <i>ipv4-address</i>   <i>host-name</i> } [ <i>port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> 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.
<b>Step 2</b>	<b>telnet6</b> { <i>ipv6-address</i>   <i>host-name</i> } [ <i>port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> 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**

[Enabling the Telnet Server](#), on page 21

## Clearing 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**

	Command or Action	Purpose
<b>Step 1</b>	<b>show users</b> <b>Example:</b> switch# show users	Displays user session information.
<b>Step 2</b>	<b>clear line vty-line</b> <b>Example:</b> switch(config)# clear line pts/12	Clears a user Telnet session.

## Verifying the SSH and Telnet Configuration

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

Command	Purpose
<b>show ssh key [dsa   rsa] [md5]</b>	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 <b>md5</b> option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.
<b>show running-config security [all]</b>	Displays the SSH and user account configuration in the running configuration. The <b>all</b> keyword displays the default values for the SSH and user accounts.
<b>show ssh server</b>	Displays the SSH server configuration.
<b>show telnet server</b>	Displays the Telnet server configuration.
<b>show username username keypair</b>	Displays the public key for the specified user.
<b>show user-account</b>	Displays configured user account details.
<b>show users</b>	Displays the users logged into the device.

Command	Purpose
<code>show crypto ca certificates</code>	Displays the configured CA certificate and associated trustpoint for X.509v3 certificate-based SSH authentication.
<code>show crypto ca crl trustpoint</code>	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(config)# show ssh key
could not retrieve dsa key information
*****
rsa Keys generated:Tue Mar 14 13:13:47 2017

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDh4+DZboQJbJt10nJhgKBYL5l0lhsFM2oZRi9+JqEU
GA44I9ej+E5NIRZ1x8ohIt6Vx9Et5cs07Pw72rjUwR3UPmuAm79k7I/SyLGEP3WUL7sqbLvNF5GqKXph
oqMT075WUdbGWphorA2g0tTObrFIQBjVQ0SSBh3oEaaALqYUQ==

bitcount:1024
fingerprint:
SHA256:V6KAeLAIKRRUPBZm1Yq3r16JW7Eo7vhLi6CXyxnD/+Y
*****
*****
```



**Step 5** Specify the SSH public key in OpenSSH format.

**Example:**

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK30iW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKu1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXY/G+1JNlQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tp1x8=
```

**Step 6** Save the configuration.

**Example:**

```
switch(config)# 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(config)# show username admin keypair

*****

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

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByYPDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFMICZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2: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(config)# 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:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2: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:



**Note** Remote TACACS authentication is not supported. Only SSH v509v3 certificate based authentication is supported.

```

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=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D: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:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78: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

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

**Related Documents**

Related Topic	Document Title
Cisco NX-OS licensing	<i>Cisco NX-OS Licensing Guide</i>
VRF configuration	<i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i>

**RFCs**

RFCs	Title
<a href="#">RFC 6187</a>	<i>X.509v3 Certificates for Secure Shell Authentication</i>

**MIBs**

MIBs	MIBs Link
MIBs related to SSH and Telnet	To locate and download supported MIBs, go to the following URL: <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>