



# Configuring SSH and Telnet

---

This chapter contains the following sections:

- [Configuring SSH and Telnet, on page 1](#)

## Configuring SSH and Telnet

### Information About SSH and Telnet

#### SSH Server

The Secure Shell Protocol (SSH) server feature enables a SSH client to make a secure, encrypted connection to a Cisco Nexus device. SSH uses strong encryption for authentication. The SSH server in the Cisco Nexus device switch interoperates with publicly and commercially available SSH clients.

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

#### SSH Client

The SSH client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a switch to make a secure, encrypted connection to another Cisco Nexus device or to any other device running an 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 Nexus device works with publicly and commercially available SSH servers.

#### SSH Server Keys

SSH requires server keys for secure communications to the Cisco Nexus device. You can use SSH 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)

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 three 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.

By default, the Cisco Nexus device generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)


**Caution**

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

## 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 system to the other. Telnet can accept either an IP address or a domain name as the remote system address.

The Telnet server is enabled by default on the Cisco Nexus device.

## Guidelines and Limitations for SSH

SSH has the following configuration guidelines and limitations:

- The Cisco Nexus device supports only SSH version 2 (SSHv2).

## Configuring 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>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>ssh key {dsa [force]   rsa [bits [force]]}</b>	Generates the SSH server key.  The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 2048 and the default value is 1024.

	Command or Action	Purpose
		Use the <b>force</b> keyword to replace an existing key.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 4</b>	(Optional) switch# <b>show ssh key</b>	Displays the SSH server keys.
<b>Step 5</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

### Example

The following example shows how to generate an SSH server key:

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

## 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 three different formats:

- Open SSH format
- IETF SECSH format
- Public Key Certificate in PEM format

### Specifying the SSH Public Keys in Open SSH Format

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

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>username <i>username</i> sshkey <i>ssh-key</i></b>	Configures the SSH public key in SSH format.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 4</b>	(Optional) switch# <b>show user-account</b>	Displays the user account configuration.
<b>Step 5</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Example**

The following example shows how to specify an SSH public key in open SSH format:

```
switch# configure terminal

switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=

switch(config)# exit

switch# show user-account

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



**Note** The **username** command in the example above is a single line that has been broken for legibility.

**Specifying the SSH Public Keys in IETF SECSH Format**

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>copy server-file bootflash: filename</b>	Downloads the file that contains the SSH key in IETF SECSH format from a server. The server can be FTP, SCP, SFTP, or TFTP.
<b>Step 2</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 3</b>	switch(config)# <b>username username sshkey file filename</b>	Configures the SSH public key in SSH format.
<b>Step 4</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 5</b>	(Optional) switch# <b>show user-account</b>	Displays the user account configuration.
<b>Step 6</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Example**

The following example shows how to specify the SSH public key in the IETF SECSH format:

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

switch# configure terminal

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

```
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

## Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

You can specify the SSH public keys in PEM-formatted Public Key Certificate form for user accounts.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>copy</b> <i>server-file</i> <b>bootflash:</b> <i>filename</i>	Downloads the file that contains the SSH key in PEM-formatted Public Key Certificate form from a server. The server can be FTP, SCP, SFTP, or TFTP
<b>Step 2</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 3</b>	(Optional) switch# <b>show user-account</b>	Displays the user account configuration.
<b>Step 4</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

### Example

The following example shows how to specify the SSH public keys in PEM-formatted public key certificate form:

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

## Starting SSH Sessions to Remote Devices

You can start SSH sessions to connect to remote devices from your Cisco Nexus device.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>ssh</b> { <i>hostname</i>   <i>username@hostname</i> } [ <b>vrf</b> <i>vrf-name</i> ]	Creates an SSH session to a remote device. The <i>hostname</i> argument can be an IPv4 address, an IPv6 address, or a hostname.

## Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, you establish a trusted SSH relationship with that server.

**Procedure**

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

**Disabling the SSH Server**

By default, the SSH server is enabled on the Cisco Nexus device.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>no feature ssh</b>	Disables the SSH server. The default is enabled.
<b>Step 3</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 4</b>	(Optional) switch# <b>show ssh server</b>	Displays the SSH server configuration.
<b>Step 5</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Deleting SSH Server Keys**

You can delete SSH server keys 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>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>no feature ssh</b>	Disables the SSH server.
<b>Step 3</b>	switch(config)# <b>no ssh key [dsa   rsa]</b>	Deletes the SSH server key. The default is to delete all the SSH keys.
<b>Step 4</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 5</b>	(Optional) switch# <b>show ssh key</b>	Displays the SSH server configuration.
<b>Step 6</b>	(Optional) switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

## Clearing SSH Sessions

You can clear SSH sessions from the Cisco Nexus device.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>show users</b>	Displays user session information.
<b>Step 2</b>	switch# <b>clear line vty-line</b>	Clears a user SSH session.

## Configuration Examples for SSH

The following example shows how to configure SSH:

### Procedure

**Step 1** Generate an SSH server key.

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

**Step 2** Enable the SSH server.

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

**Note** This step should not be required because the SSH server is enabled by default.

**Step 3** Display the SSH server key.

```
switch(config)# show ssh key
rsa Keys generated:Fri May 8 22:09:47 2009

ssh-rsa
AAAAB3NzaClyc2EAAAABlwAAAEArI3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*****
could not retrieve dsa key information
```

```
*****
```

**Step 4** Specify the SSH public key in Open SSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CftPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

**Step 5** Save the configuration.

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

## Configuring Telnet

### Enabling the Telnet Server

By default, the Telnet server is enabled. You can disable the Telnet server on your Cisco Nexus device.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>feature telnet</b>	Disables the Telnet server. The default is enabled.

### Reenabling the Telnet Server

If the Telnet server on your Cisco Nexus device has been disabled, you can reenabling it.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch(config)# <b>feature telnet</b>	Reenables the Telnet server.

## Starting Telnet Sessions to Remote Devices

Before you start a Telnet session to connect to remote devices, you should do the following:

- Obtain the hostname for the remote device and, if needed, obtain the username on the remote device.
- Enable the Telnet server on the Cisco Nexus device.
- Enable the Telnet server on the remote device.



**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>telnet</b> <i>hostname</i>	Creates a Telnet session to a remote device. The <i>hostname</i> argument can be an IPv4 address, an IPv6 address, or a device name.

**Example**

The following example shows how to start a Telnet session to connect to a remote device:

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

**Clearing Telnet Sessions**

You can clear Telnet sessions from the Cisco Nexus device.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>show users</b>	Displays user session information.
<b>Step 2</b>	switch# <b>clear line</b> <i>vtty-line</i>	Clears a user Telnet session.

**Verifying the SSH and Telnet Configuration**

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

**Procedure**

- switch# **show ssh key** [**dsa** | **rsa**]  
Displays SSH server key-pair information.
- switch# **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.
- switch# **show ssh server**  
Displays the SSH server configuration.
- switch# **show user-account**  
Displays user account information.

## Default Settings for SSH

The following table lists the default settings for SSH parameters.

*Table 1: Default SSH Parameters*

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Enabled