



CHAPTER 5

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:

- [Information About SSH and Telnet, page 5-1](#)
- [Licensing Requirements for SSH and Telnet, page 5-3](#)
- [Prerequisites for SSH, page 5-3](#)
- [Guidelines and Limitations, page 5-3](#)
- [Configuring SSH, page 5-3](#)
- [Configuring Telnet, page 5-11](#)
- [Verifying the SSH and Telnet Configuration, page 5-14](#)
- [SSH Example Configuration, page 5-14](#)
- [Default Settings, page 5-15](#)
- [Additional References, page 5-15](#)

Information About SSH and Telnet

This section includes the following topics:

- [SSH Server, page 5-1](#)
- [SSH Client, page 5-2](#)
- [SSH Server Keys, page 5-2](#)
- [Telnet Server, page 5-2](#)
- [Virtualization Support, page 5-3](#)

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.

Send document comments to nexus7k-docfeedback@cisco.com

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, 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)

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 two 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 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.

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 NX-OS device.

Send document comments to nexus7k-docfeedback@cisco.com

Virtualization Support

SSH and Telnet configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*.

Licensing Requirements for SSH and Telnet

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	SSH and Telnet require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

Prerequisites for SSH

SSH and Telnet have the following prerequisites:

- 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

SSH and Telnet have the following configuration guidelines and limitations:

- The Cisco NX-OS software supports only SSH version 2 (SSHv2).



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.

Configuring SSH

This section includes the following sections:

- [Generating SSH Server Keys, page 5-4](#)
- [Specifying the SSH Public Keys for User Accounts, page 5-5](#)
- [Starting SSH Sessions, page 5-7](#)
- [Clearing SSH Hosts, page 5-8](#)
- [Disabling the SSH Server, page 5-8](#)
- [Deleting SSH Server Keys, page 5-9](#)
- [Clearing SSH Sessions, page 5-10](#)

Send document comments to nexus7k-docfeedback@cisco.com

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.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **no ssh server enable**
3. **ssh key {dsa [force] | rsa [bits [force]]}**
4. **ssh server enable**
5. **exit**
6. **show ssh key**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	no ssh server enable Example: switch(config)# no ssh server enable	Disables SSH.
Step 3	ssh key {dsa [force] rsa [bits [force]]} Example: switch(config)# ssh key rsa 2048	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. Use the force keyword to replace an existing key.
Step 4	ssh server enable Example: switch(config)# ssh server enable	Enables SSH.
Step 5	exit Example: switch(config)# exit switch#	Exits global configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com

	Command	Purpose
Step 6	show ssh key Example: switch# show ssh key	(Optional) Displays the SSH server keys.
Step 7	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) 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
- Public Key Certificate in PEM format

Specifying the SSH Public Keys in OpenSSH Format

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).
Generate an SSH public key in OpenSSH format.

SUMMARY STEPS

1. **config t**
2. **username *username* sshkey *ssh-key***
3. **exit**
4. **show user-account**
5. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	username username sshkey ssh-key Example: switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1X swK3Oiw4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/ DQhum+lJNqJP/eLowb7ubO+lVKRXYF/G+lJNlQW3g9igG 30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH 3UD/vKyziEh5S4Tplx8=	Configures the SSH public key in OpenSSH format.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	show user-account Example: switch# show user-account	(Optional) Displays the user account configuration.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

You have generated an SSH public key in IETF SCHSH format.

SUMMARY STEPS

1. **copy server-file bootflash:filename**
2. **config t**
3. **username username sshkey file bootflash:filename**
4. **exit**
5. **show user-account**
6. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	copy <i>server-file</i> bootflash: <i>filename</i> 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	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 3	username <i>username</i> sshkey file bootflash: <i>filename</i> 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	show user-account Example: switch# show user-account	(Optional) Displays the user account configuration.
Step 6	copy running-config startup-config Example: switch# 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.

SUMMARY STEPS

1. **ssh** [*username@*]{*hostname* | *username@hostname*} [**vrf** *vrf-name*]
ssh6 [*username@*]{*hostname* | *username@hostname*} [**vrf** *vrf-name*]

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	<pre>ssh [username@]{ipv4-address hostname} [vrf vrf-name]</pre> <p>Example: switch# ssh 10.10.1.1</p>	Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.
	<pre>ssh6 [username@]{ipv6-address hostname} [vrf vrf-name]</pre> <p>Example: switch# ssh6 HostA</p>	Creates an SSH IPv6 session to a remote device using IPv6.

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.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. clear ssh hosts

DETAILED STEPS

	Command	Purpose
Step 1	<pre>clear ssh hosts</pre> <p>Example: switch# clear ssh hosts</p>	Clears the SSH host sessions.

Disabling the SSH Server

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. config t
2. no ssh server enable

Send document comments to nexus7k-docfeedback@cisco.com

3. `exit`
4. `show ssh server`
5. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: switch# <code>config t</code> switch(config)#	Enters global configuration mode.
Step 2	<code>no ssh server enable</code> Example: switch(config)# <code>no ssh server enable</code>	Disables the SSH server. The default is enabled.
Step 3	<code>exit</code> Example: switch(config)# <code>exit</code> switch#	Exits global configuration mode.
Step 4	<code>show ssh server</code> Example: switch# <code>show ssh server</code>	(Optional) Displays the SSH server configuration.
Step 5	<code>copy running-config startup-config</code> Example: switch# <code>copy running-config startup-config</code>	(Optional) 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 reenab SSH, you must first generate an SSH server key (see the [“Generating SSH Server Keys”](#) section on page 5-4).

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the `switchto vdc` command).

SUMMARY STEPS

1. `config t`
2. `no ssh server enable`
3. `no ssh key [dsa | rsa]`
4. `exit`
5. `show ssh key`

Send document comments to nexus7k-docfeedback@cisco.com

6. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: switch# <code>config t</code> switch(config)#	Enters global configuration mode.
Step 2	<code>no ssh server enable</code> Example: switch(config)# <code>no ssh server enable</code>	Disables the SSH server.
Step 3	<code>no ssh key [dsa rsa]</code> Example: switch(config)# <code>no ssh key rsa</code>	Deletes the SSH server key. The default is to delete all the SSH keys.
Step 4	<code>exit</code> Example: switch(config)# <code>exit</code> switch#	Exits global configuration mode.
Step 5	<code>show ssh key</code> Example: switch# <code>show ssh key</code>	(Optional) Displays the SSH server key configuration.
Step 6	<code>copy running-config startup-config</code> Example: switch# <code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

Clearing SSH Sessions

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the `switchto vdc` command).

SUMMARY STEPS

1. `show users`
1. `clear line vty-line`

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

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

Configuring Telnet

This section includes the following topics:

- [Enabling the Telnet Server, page 5-11](#)
- [Starting Telnet Sessions to Remote Devices, page 5-12](#)
- [Clearing Telnet Sessions, page 5-13](#)

Enabling the Telnet Server

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **telnet server enable**
3. **exit**
4. **show telnet server**
5. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.
Step 2	telnet server enable Example: switch(config)# telnet server enable	Enables the Telnet server. The default is disabled.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	show telnet server Example: switch# show telnet server	(Optional) Displays the Telnet server configuration.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) 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 , in Cisco NX-OS Release 4.0(2) and later releases, 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 NX-OS device (see the [“Enabling the Telnet Server”](#) section on page 5-11).

Enable the Telnet server on the remote device.

SUMMARY STEPS

1. **telnet** {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]
telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	telnet { <i>ipv4-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] 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.
	telnet6 { <i>ipv6-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] Example: switch# telnet 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. Note Cisco NX-OS Release 4.0(2) and later releases support IPv6 for starting Telnet session.

Clearing Telnet Sessions

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Enable the Telnet server on the NX-OS device.

SUMMARY STEPS

1. **show users**
2. **clear line** *vti-line*

DETAILED STEPS

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

Send document comments to nexus7k-docfeedback@cisco.com

Verifying the SSH and Telnet Configuration

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

Command	Purpose
<code>show ssh key [dsa rsa]</code>	Displays SSH server key-pair information.
<code>show running-config security [all]</code>	Displays the SSH and user account configuration in the running configuration. The all keyword displays the default values for the SSH and user accounts.
<code>show ssh server</code>	Displays the SSH server configuration.
<code>show telnet server</code>	Displays the SSH server configuration.

For detailed information about the fields in the output from these commands, see the [Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0](#).

SSH Example Configuration

To configure SSH with an OpenSSH key, follow these steps:

Step 1 Disable the SSH server.

```
switch# config t
switch(config)# no ssh server enable
```

Step 2 Generate an SSH server key.

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

Step 3 Enable the SSH server.

```
switch(config)# ssh server enable
```

Step 4 Display the SSH server key.

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWheBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svrWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K361r39HmXL6VgprVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmm4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*****
could not retrieve dsa key information
*****
```

Send document comments to nexus7k-docfeedback@cisco.com

Step 5 Specify the SSH public key in OpenSSH format.

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZ19G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+1JNqJP/eLowb7ubO+1VKRXYF/G+1JNlQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tp1x8=
```

Step 6 Save the configuration.

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

Default Settings

Table 5-1 lists the default settings for SSH and Telnet parameters.

Table 5-1 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.

Additional References

For additional information related to implementing RBAC, see the following sections:

- [Related Documents, page 5-15](#)
- [Standards, page 5-16](#)
- [MIBs, page 5-16](#)

Related Documents

Related Topic	Document Title
Licensing	<i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0</i>
VRF configuration	<i>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0</i>

Send document comments to nexus7k-docfeedback@cisco.com

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none">CISCO-SECURE-SHELL-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml