Configure Secure Shell

Note Starting with, Secure Shell Version 1 (SSHv1) is deprecated.

- SSH, on page 1

SSH

A secure shell (SSH) protocol is a network security mechanism that

- establishes encrypted and authenticated connections between remote devices. and
- protects data confidentiality and integrity during communication.
- supports multiple version standards, including SSHv1 and SSHv2.

How SSH sorks and security benefits

Secure Shell (SSH) protocols offer a secure alternative to older remote access methods, such as Telnet, by encrypting data exchanged between a client and a server. Authentication further ensures that only authorized users can access devices. SSH increases security for network administrators by preventing eavesdropping and protecting credentials.

- Connecting securely to a router or switch for remote configuration.
- Transferring files securely between devices using SCP, which operates over SSH.

SSH and device access

A Secure Shell (SSH) protocol is a network access method that

- uses strong encryption and authentication to secure remote connections
- offers enhanced security over Telnet by encrypting session and authentication data, and
- supports both IPv4 and IPv6 environments for flexible device access.

Additional information

SSH is a secure protocol for remote device access, supporting both IPv4 and IPv6, and provides strong encryption for authenticated sessions.

SSH servers and integrated clients

A SSH integrated client is a feature that - runs over the SSH protocol to provide device authentication - enables secure, encrypted connections to other devices, and - supports various user authentication methods.

Supported versions and functionalities

The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server.

This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted.

With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

Note The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

SSH configuration guidelines

General SSH configuration guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on an active switch and the active switch fails, the new active switch uses the RSA key pair generated by the previous active switch.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command.

- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

SCP

A Secure Copy Protocol is a method for securely transferring files that

- provides a secure and authenticated method for copying switch configurations or switch image files
- relies on Secure Shell (SSH) for secure transport, and
- requires correct configuration of SSH, authentication, and authorization on the switch.

Supporting reference information

For SSH to work, the switch needs an RSA public or private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have a Rivest, Shamir, and Adelman (RSA) key pair.

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure copy protocol

A Secure Copy Protocol is a network protocol that

- provides a secure and authenticated method for copying files
- relies on SSH for security, and
- requires authentication, authorization, and accounting (AAA) authorization.

Additional information on SCP

The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite.

To configure the SCP, you should understand the SCP concepts.

SFTP support

SFTP client support is introduced from Cisco IOS XE Gibraltar 16.10.1 release onwards. SFTP client is enabled by default and no separate configuration required. The SFTP procedures can be invoked using the **copy** command, which is similar to that of **scp** and **tftp** commands. A typical file download procedure using **sftp** command can be carried out as shown below:

copy sftp://*user* :*password @server-ip*/*file-name* **flash0://** *file-name*

For more details on the **copy** command, see the following URL:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

Prerequisites for configuring SSH

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.
- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

Restrictions for configuring SSH

These are restrictions for configuring the device for secure shell.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. However, you can add them manually if required. For information on manually adding these algorithms, see the https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html.
- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.

- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The device supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.
- To authenticate clients with FreeRADIUS over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *label-name* command to achieve this.

Set up the device to run SSH

Enable SSH on the device for secure remote access.

Follow the procedure given below to set up your device to run SSH:

Before you begin

Configure user authentication for local or remote access.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the hostname and IP domain name for your device.

Example:

```
Device(config)# hostname your_hostname
```

Note
Follow this procedure only if you are configuring the device as an SSH server.

Step 3 Configure a host domain for your device.

Example:

```
Device(config)# ip domain name your_domain
```

Step 4 Enable the SSH server and generate an RSA key pair.

Example:

```
Device(config)# crypto key generate rsa
```

Generating an RSA key pair for the device automatically enables SSH.

We recommend that a minimum modulus size of 1024 bits.

When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.

Note
Follow this procedure only if you are configuring the device as an SSH server.

Step 5 Exit configuration mode.

Example:

```
Device(config)# end
```

The device is now set up to run SSH, allowing secure remote access.

Configure the SSH server

Set up the SSH server to allow secure remote access to the device.

Follow the procedure given below to configure the SSH server:

Note This procedure is only required if you are configuring the device as an SSH server.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 (Optional) Configure the device to run SSH Version 2.

Example:

```
Device(config)# ip ssh version 2
```

If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client.

Step 3 Configure the SSH control parameters.

Example:

```
Device(config)# ip ssh timeout
seconds
authentication-retries
number
```

Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase.

By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4).

Step 4 (Optional) Use one or both of the following:

- `line vty` *line_number* [*ending_line_number*]
- **transport input ssh**

Example:

```
Device(config)# line vty
line-number
ending-line-number
```

or

```
Device(config-line)# transport input ssh
```

Enters line configuration mode to configure the virtual terminal line settings. For *line-number* and *ending-line-number* , specify a pair of lines. The range is 0 to 15.

Specifies that the device prevent non-SSH Telnet connections. This limits the router to only SSH connections.

Note
If the Virtual Terminal (VTY) lines are exhausted, Telnet or SSH will fail. You can either disconnect the Telnet or SSH sessions to free up the VTY lines, or follow the recovery steps given below to clear VTY lines and reload Telnet or SSH:

```
Device# configure terminal
Device(config)# clear line
line number
```

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-line)# end
```

Returns to privileged EXEC mode.

The SSH server is now configured and ready for secure remote access.

Monitor the SSH configuration and status

This table displays the SSH server configuration and status.

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.