



## Secure Shell Commands

---

This chapter describes Secure Shell (SSH) commands. SSH is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures the remote connection to a router using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley **rexec** and **rsh** tools. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

To find complete descriptions of other commands used when configuring SSH, refer to the *Cisco IOS Command Reference Master Index* or search online.

For SSH configuration information, refer to the “Configuring Secure Shell” chapter in the *Cisco IOS Security Configuration Guide*.

# disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** privileged EXEC command.

```
disconnect ssh [vty] session-id
```

Syntax Description	vtty	(Optional) Virtual terminal for remote console access.
	<i>session-id</i>	The session-id is the number of connection displayed in the <b>show ip ssh</b> command output.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.

Usage Guidelines	The <b>clear line vty n</b> command, where <i>n</i> is the connection number displayed in the <b>show ip ssh</b> command output, may be used instead of the <b>disconnect ssh</b> command.
------------------	--

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples	The following example terminates SSH connection number 1:
----------	---

```
disconnect ssh 1
```

Related Commands	Command	Description
	<b>clear line vty</b>	Returns a terminal line to idle state using the privileged EXEC command.

# ip scp server enable

To enable secure copy (SCP) server-side functionality, use the **ip scp server enable** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip scp server enable**

**no ip scp server enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command is disabled by default.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S and implemented on the following platforms: Cisco 7500 series and Cisco 12000 series.

**Usage Guidelines** Use the **ip scp server enable** command to enable a Cisco router to support SCP server-side functionality, which allows an authenticated user to securely copy configuration and image files to or from a remote workstation.

Before a user can utilize the SCP server-side functionality, Secure Shell (SSH), authentication, and authorization must be properly configured so that a router can determine whether a user is at the correct privilege level.

**Examples** The following example shows how to transfer a file from the router using SCP:

```
Router# copy flash:c3620-ik9s-mz.122-0.17.T scp://tiger@10.1.1.2/  
Address or name of remote host [10.1.1.2]?  
Destination username [tiger]?  
Destination filename [c3620-ik9s-mz.122-0.17.T]?  
Writing c3620-ik9s-mz.122-0.17.T  
Password:
```

Router#



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

**ip scp server enable****Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa authentication login</b>	Sets AAA authentication at login.
<b>aaa authorization</b>	Sets parameters that restrict user access to a network.
<b>copy</b>	Copies any file from a source to a destination.
<b>username</b>	Establishes a username-based authentication system.

# ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** global configuration command. To restore the default value, use the **no** form of this command.

```
ip ssh {[timeout seconds]} | [authentication-retries integer]}
```

```
no ip ssh {[timeout seconds]} | [authentication-retries integer]}
```

## Syntax Description

<b>timeout</b>	(Optional) The time interval that the router waits for the SSH client to respond.  This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
<b>authentication-retries</b>	(Optional) The number of attempts after which the interface is reset.
<i>seconds</i>	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
<i>integer</i>	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

## Defaults

120 seconds for the timeout timer.  
3 authentication-retries.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.

## Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

## Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

# ip ssh port

To enable secure access to tty (asynchronous) lines, use the **ip ssh port** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip ssh port** *portnum* **rotary** *group*

**no ip ssh port** *portnum* **rotary** *group*

## Syntax Description

<i>portnum</i>	Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.
<b>rotary</b> <i>group</i>	Specifies the defined rotary that should search for a valid name.

## Defaults

This command is disabled by default.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(2)T	This command was introduced.

## Usage Guidelines

The **ip ssh port** command supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

## Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
  no exec
  login authentication default
  rotary 1
  transport input ssh
  exit
ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```

line 1
  no exec
  login authentication default
  rotary 1
  transport input ssh
line 2
  no exec
  login authentication default
  rotary 2
  transport input ssh
line 3
  no exec
  login authentication default
  rotary 3
  transport input ssh
  exit
ip ssh port 2001 rotary 1 3

```

From any UNIX or UNIX-like device, the following command is typically used to form an SSH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the 3DES cipher to the device known as “router.example.com,” which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

#### Related Commands

Command	Description
<b>ip ssh</b>	Configures SSH control variables on your router.
<b>line</b>	Identifies a specific line for configuration and begins the command in line configuration mode.
<b>rotary</b>	Defines a group of lines consisting of one or more lines.
<b>ssh</b>	Starts an encrypted session with a remote networking device.
<b>transport input</b>	Defines which protocols to use to connect to a specific line of the router.

# show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** privileged EXEC command.

**show ip ssh**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
	12.1(5)T	This command was modified to display the SSH status—enabled or disabled.

**Usage Guidelines** Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

**Examples** The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following is sample output from the **show ip ssh** command when SSH has been disabled:

```
Router# show ip ssh

%SSH has not been enabled
```

Related Commands	Command	Description
	<a href="#">show ssh</a>	Displays the status of SSH server connections.

# show ssh

To display the status of Secure Shell (SSH) server connections, use the **show ssh** privileged EXEC command.

**show ssh**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

**Usage Guidelines** Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data; use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

**Examples** The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh

Connection      Version      Encryption      State           Username
0               1.5         3DES           Session Started guest
```

The following is sample output from the **show ssh** command with SSH disabled:

```
Router# show ssh
%No SSH server connections running.
```

Related Commands	Command	Description
	<a href="#">show ip ssh</a>	Displays the version and configuration data for SSH.

# ssh

To start an encrypted session with a remote networking device, use the **ssh** user EXEC command.

```
ssh [-l userid] [-c {des | 3des}] [-o numberofpasswordprompts n] [-p portnum] {ipaddr | hostname}
    [command]
```

Syntax Description	
<b>-l</b> <i>userid</i>	(Optional) Specifies the user ID to use when logging in as on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
<b>-c</b> { <b>des</b>   <b>3des</b> }	(Optional) Specifies the crypto algorithm, DES or 3DES, to use for encrypting data. To use SSH, you must have an encryption image must be running on the router. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES).
<b>-o</b> <b>numberofpasswordprompts</b> <i>n</i>	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the <b>-o numberofpasswordprompts</b> keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
<b>-p</b> <i>portnum</i>	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
<i>address</i>   <i>hostname</i>	Specifies the IPv4 or IPv6 address or host name of the remote networking device.
<i>command</i>	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(8)T, 12.0(21)ST, 12.0(22)S	Suuport for IPv6 addresses was added.

**Usage Guidelines**

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

**Note**

SSH is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

The **ssh** command requires that you first enable the SSH server on the router. The SSH client is available only when the SSH server is enabled.

**Examples**

The following example illustrates initiating a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates initiating a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for this to work.

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 3ffe:1111:2222:1044::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

**Note**

A host name that maps to the IPv6 address 3ffe:1111:2222:1044::72 could have been used in the last example.

**Related Commands**

Command	Description
<a href="#">ip ssh</a>	Configures SSH server control parameters on the router.
<a href="#">show ip ssh</a>	Displays the version and configuration data for SSH.
<a href="#">show ssh</a>	Displays the status of SSH server connections.

