



Secure Shell Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure Secure Shell (SSH). For detailed information about SSH concepts, configuration tasks, and examples, see the *Implementing Secure Shell on Cisco IOS XR Software* configuration module.

clear ssh

To terminate an incoming or outgoing Secure Shell (SSH) connection, use the **clear ssh** command in EXEC mode.

```
clear ssh {session-id | outgoing session-id}
```

Syntax Description		
	<i>session-id</i>	Session ID number of an incoming connection as displayed in the show ssh command output. Range is from 0 to 1024.
	outgoing <i>session-id</i>	Specifies the session ID number of an outgoing connection as displayed in the show ssh command output. Range is from 1 to 10.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear ssh** command to disconnect incoming or outgoing SSH connections. Incoming connections are managed by the SSH server running on the local networking device. Outgoing connections are initiated from the local networking device.

To display the session ID for a connection, use the **show ssh** command.

Examples

In the following example, the **show ssh** command is used to display all incoming and outgoing connections to the router. The **clear ssh** command is then used to terminate the incoming session with the ID number 0.

```
RP/0/RP0/CPU0:router# show ssh

SSH version: Cisco-2.0
session  pty    location  state      userid    host      ver
-----
Incoming sessions
0        vty0    0/33/1    SESSION_OPEN  cisco    172.19.72.182  v2
1        vty1    0/33/1    SESSION_OPEN  cisco    172.18.0.5     v2
2        vty2    0/33/1    SESSION_OPEN  cisco    172.20.10.3    v1
3        vty3    0/33/1    SESSION_OPEN  cisco    3333:::50     v2

Outgoing sessions
1                0/33/1    SESSION_OPEN  cisco    172.19.72.182  v2
2                0/33/1    SESSION_OPEN  cisco    3333:::50     v2

RP/0/RP0/CPU0:router# clear ssh 0
```

Related Commands

Command	Description
show ssh	Displays the incoming and outgoing connections to the router.

sftp

To copy files to and from a router, use the **sftp** command in EXEC mode.

```
sftp [[username@]hostname:]srcfile [[[[username@]hostname:]srcfile...] | source-interface type instance | dstfile]
```

Syntax Description

<i>username</i>	(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.
<i>hostname</i>	(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.
srcfile	SFTP source, including the path.
source-interface <i>type</i> instance	(Optional) Source IP address of a selected interface for all outgoing SSH connections. Interface type. For more information, use the question mark (?) online help function. Either a physical interface instance or a virtual interface instance as follows: <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>dstfile</i>	SFTP destination, including the path.

Defaults

If no *username* argument is provided, the login name on the router is used. If no *host name* argument is provided, the file is considered local.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SFTP provides for the secure (and authenticated) copying of files between a router and a remote host. Like the **copy** command, the **sftp** command can be invoked only in EXEC mode.

If a username is not provided, the login name on the router is used as the default. If a host name is not provided, the file is considered local.

If the source-interface is specified in the **sftp** command, the **sftp** interface takes precedence over the interface specified in the **ssh client source-interface** command.

When the file destination is a local path, all of the source files should be on remote hosts, and vice versa.

When multiple source files exist, the destination should be a preexisting directory. Otherwise, the destination can be either a directory name or destination filename. The file source cannot be a directory name.

If you download files from different remote hosts, that is, the source points to different remote hosts, the SFTP client spawns SSH instances for each host, which may result in multiple prompts for user authentication.

Examples

In the following example, user *abc* is downloading the file *ssh.diff* from the SFTP server *ena-view1* to *disk0*:

```
RP/0/RP0/CPU0:router# sftp abc@ena-view1:ssh.diff disk0
```

In the following example, user *abc* is uploading multiple files from *disk 0:/sam_** to */users/abc/* on a remote SFTP server called *ena-view1*:

```
RP/0/RP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

Related Commands

Command	Description
ssh client source-interface	Specifies the source IP address of a selected interface for all outgoing SSH connections.

show ssh

To display all incoming and outgoing connections to the router, use the **show ssh** command in EXEC mode.

show ssh

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ssh** command to display all incoming and outgoing Secure Shell (SSH) Version 1 (SSHv1) and SSH Version 2 (SSHv2) connections.

Examples

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

```
RP/0/RP0/CPU0:router# show ssh

SSH version: Cisco-2.0

id pty      location  state      userid    host      ver
-----
Incoming sessions

0 vty0      0/0/CPU0  SESSION_OPEN  cisco     172.19.72.182  v2
1 vty1      0/0/CPU0  SESSION_OPEN  cisco     172.18.0.5     v2
2 vty2      0/0/CPU0  SESSION_OPEN  cisco     172.20.10.3   v1
3 vty3      0/0/CPU0  SESSION_OPEN  cisco     3333::50      v2

Outgoing sessions

1          0/0/CPU0  SUSPENDED    root      172.19.72.182  v2
```

Table 13 describes the significant fields shown in the display.

Table 13 *show ssh Field Descriptions*

Field	Description
session	Session identifier for the incoming and outgoing SSH connections.
pty	pty-id allocated for the incoming session. Null for outgoing SSH connection.
location	Specifies where the SSH server is running for incoming connection. For an outgoing connection, location specifies from which route processor the SSH session is initiated.
state	The SSH state that the connection is currently in.
userid	Authentication, authorization and accounting (AAA) username used to connect to or from the router.
host	IP address of the remote peer.
ver	Specifies if the connection type is SSHv1 or SSHv2.

Related Commands

Command	Description
show session	Displays information about open Telnet or rlogin connections.
show ssh session details	Displays the details for all the incoming and outgoing SSHv2 connections to the router.
show user	Displays information about the active lines on the router.

show ssh session details

To display the details for all incoming and outgoing Secure Shell Version 2 (SSHv2) connections, use the **show ssh session details** command in EXEC mode.

show ssh session details

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ssh session details** command to display a detailed report of the SSHv2 connections to or from the router, including the cipher chosen for the specific session.

Examples The following sample output is from the **show ssh session details** command to display the details for all the incoming and outgoing SSHv2 connections:

```
RP/0/RP0/CPU0:router# show ssh session details
```

```
SSH version: Cisco-2.0
session    key-exchange    pubkey    incipher    outcipher    inmac    outmac
-----
Incoming Session
0          diffie-hellman  ssh-dss   3des-cbc   3des-cbc    hmac-md5  hmac-md5

Outgoing connection
1          diffie-hellman  ssh-dss   3des-cbc   3des-cbc    hmac-md5  hmac-md5
```

Table 14 describes the significant fields shown in the display.

Table 14 *show ssh session details Field Descriptions*

Field	Description
session	Session identifier for the incoming and outgoing SSH connections.
key-exchange	Key exchange algorithm chosen by both peers to authenticate each other.
pubkey	Public key algorithm chosen for key exchange.
incipher	Encryption cipher chosen for the Rx traffic.
outcipher	Encryption cipher chosen for the Tx traffic.
inmac	Authentication (message digest) algorithm chosen for the Rx traffic.
outmac	Authentication (message digest) algorithm chosen for the Tx traffic.

Related Commands

Command	Description
show session	Displays information about open Telnet or rlogin connections.
show ssh	Displays all the incoming and outgoing connections to the router.
show user	Displays information about the active lines on the router.

ssh

To enable an outbound Secure Shell (SSH) client connection, use the **ssh** command in EXEC mode.

```
ssh {ipv4-address | ipv6-address | hostname} [username user-id | cipher des | source-interface type instance]
```

Syntax Description

ipv4-address	IPv4 address in four-part dotted-decimal notation.
ipv6-address	IPv6 (A:B:C:D:... :D or A:B:C:D:... :P) address.
hostname	Hostname of the remote node. If the hostname has both IPv4 and IPv6 addresses, the IPv6 address is used.
username <i>user-id</i>	(Optional) Username to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
cipher des	(Optional) Cipher suite. Valid only for a Version 1 (v1) connection. Triple data encryption standard (3DES) is a default cipher suite, unless the cipher suite is specified with the cipher option. SSHv2 supports only 3DES (protocol supports only ciphers greater than or equal to 128 bits). SSHv1 supports both the DES (56-bit) and 3DES (168-bit) cipher suites.
source interface <i>type instance</i>	(Optional) Source IP address of a selected interface for all outgoing SSH connections. Either a physical interface instance or a virtual interface instance as follows: <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

Defaults No default behavior or values

Command Modes EXEC

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh** command to make an outbound client connection. The SSH client tries to make an SSHv2 connection to the remote peer. If the remote peer supports only the SSHv1 server, it internally spawns an SSHv1 connection to the remote server. The process of the remote peer version detection and spawning the appropriate client connection is transparent to the user.

If the source-interface is specified in the **ssh** command, the **ssh** interface takes precedence over the interface specified in the **ssh client source-interface** command.

The **cipher des** options can be used only with SSHv1 clients.

Examples The following sample output is from the **ssh** command to enable an outbound SSH client connection:

```
RP/0/RP0/CPU0:router# ssh remote-host username userabc
Password:
Remote-host>
```

Command	Description
show ssh	Displays all the incoming and outgoing connections to the router.

ssh client knownhost

To authenticate a server public key (pubkey), use the **ssh client knownhost** command in global configuration mode. To disable authentication of a server pubkey, use the **no** form of this command.

ssh client knownhost *device:/filename*

no ssh client knownhost *device:/filename*

Syntax Description

device:/filename Complete path of the filename (for example, slot0:/server_pubkey). The colon (:) and slash (/) are required.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh client knownhost** command to authenticate and check the server pubkey (a cryptographic system that uses two keys—a public key known to everyone and a private or secret key known only to the owner of the keys) at the client end. In the absence of certificates the server pubkey is transported to the client through an out-of-band secure channel. The client stores this pubkey in its local database and compares this key against the key supplied by the server during the early stage of key negotiation for a session-building handshake. If the key is not matched or no key is found in the client local database, the user is prompted with the warning to accept or reject this session.

The assumption in this process is that the first time the server pubkey is retrieved through an out-of-band secure channel, it is stored in the local database. This process is identical to the current model adapted by Secure Shell (SSH) implementations in the UNIX environment.

Examples

The following sample output is from the **ssh client knownhost** command:

```
RP/0/RP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RP0/CPU0:host1# exit
RP/0/RP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

To specify the source IP address of a selected interface for all outgoing Secure Shell (SSH) connections, use the **ssh client source-interface** command in global configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ssh client source-interface *type instance*

no ssh client source-interface *type instance*

Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	<p>Either a physical interface instance or a virtual interface instance as follows:</p> <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

Defaults

No source interface is used.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh client source-interface** command to set the the IP address of the specified interface for all outgoing SSH connections. If this command is not configured, TCP chooses the source IP address when the socket is connected, based on the outgoing interface used—which in turn is based on the route required to reach the server. This command applies to outbound shell over SSH as well as Secure Shell File Transfer Protocol (SFTP) sessions, which use the ssh client as a transport.

The source-interface configuration affects connections only to the remote host in the same address family. The system database (Sysdb) verifies that the interface specified in the command has a corresponding IP address (in the same family) configured.

Examples

The following example shows how to set the IP address of the Management Ethernet interface on 0/0/CPU0/0 for all outgoing SSH connections:

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# ssh client source-interface MgmtEth 0/0/CPU0/0
```

ssh server

To initiate the Security Shell (SSH) server, use the **ssh server** command in global configuration mode. To bring down an SSH server, use the **no** form of this command.

ssh server

no ssh server

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh server** command to bring an SSH server up or down.

To verify that the SSH server is up and running, use the **show process sshd** command.

The SSH server listens for an incoming client connection on port 22. This server will handle both Secure Shell Version 1 (SSHv1) and SSHv2 incoming client connections for both IPv4 and IPv6 address families.

Examples

In the following example, the SSH server is enabled:

```
RP/0/RP0/CPU0:router(config)# ssh server
```

Related Commands

Command	Description
show process sshd	Displays information about the SSH server.

ssh server rate-limit

To limit the number of incoming Secure Shell (SSH) connection requests allowed per minute, use the **ssh server rate-limit** command in global configuration mode. To return to the default value, use the **no** form of this command.

ssh server rate-limit *rate-limit*

no ssh server rate-limit

Syntax Description	<i>rate-limit</i>	Number of incoming SSH connection requests allowed per minute. Range is from 1 to 120.
---------------------------	-------------------	--

Defaults	<i>rate-limit</i> : 60 connection requests per minute
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.	
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.	

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh server rate-limit** command to limit the incoming SSH connection requests to the configured rate. Any connection request beyond the rate limit is rejected by the SSH server. Changing the rate limit does not affect established SSH sessions.

If, for example, the *rate-limit* argument is set to 30, then 30 requests are allowed per minute, or more precisely, a two-second interval between connections is enforced.

Examples The following example shows how to set the limit of incoming SSH connection requests to 20 per minute:

```
RP/0/RP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

To configure the number of allowable concurrent incoming Secure Shell (SSH) sessions, use the **ssh server session-limit** command in global configuration mode. To return to the default value, use the **no** form of this command.

ssh server session-limit *sessions*

no ssh server session-limit

Syntax Description

<i>sessions</i>	Number of incoming SSH sessions allowed across the router.
-----------------	--

Defaults

sessions: 64 per router

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ssh server session-limit** command to configure the limit of allowable concurrent incoming SSH connections. Outgoing connections are not part of the limit.

Examples

The following example shows how to set the limit of incoming SSH connections to 50:

```
RP/0/RP0/CPU0:router(config)# ssh server session-limit 50
```

ssh timeout

To configure the timeout value for authentication, authorization, and accounting (AAA) user authentication, use the **ssh timeout** command in global configuration mode. To set the timeout value to the default time, use the **no** form of this command.

ssh timeout *seconds*

no ssh timeout *seconds*

Syntax Description	<i>seconds</i> Time period (in seconds) for user authentication. The range is from 5 to 120.
---------------------------	--

Defaults	<i>seconds</i> : 30 seconds
-----------------	-----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

Use the **ssh timeout** command to configure the timeout value for user authentication to AAA. If the user fails to authenticate itself within the configured time to AAA, the connection is aborted. If no value is configured, the default value of 30 seconds is used.

Examples	In the following example, the timeout value for AAA user authentication is set to 60 seconds:
-----------------	---

```
RP/0/RP0/CPU0:router(config)# ssh timeout 60
```

