



# Configuring the Secure Shell Daemon Protocol

---

The Secure Shell Daemon (SSHD) protocol provides secure encrypted communications between two hosts communicating over an insecure network. The CSS supports an implementation of OpenSSH to provide this secure communication. SSHD uses the standard CSS login sequence of entering the username and password at the CSS login prompts.

SSHD on the CSS supports both the SSH v1 and v2 protocols. For SSH v1, the software provides encrypted communication using ciphers such as 3DES or Blowfish. For SSH v2, the software provides 128-bit AES, Blowfish, 3DES, CAST128, Arcfour, 192-bit AES, or 256-bit AES.



## Caution

When using SSHD, ensure that the CSS is not configured to perform a network boot from a network-mounted file system on a remote system (a diskless environment). If you require the CSS to use the network-mounted method of booting, be aware that the SSHD protocol is not supported.

If the CSS has been booted using a network boot from a network-mounted file system, the CSS logs the following error message by SSHD as the protocol attempts to initialize (and then exit from operation):

```
Unable to initialize sshd; failure to seed random number generator
```

---

This chapter contains the following major sections:

- [Enabling SSH](#)
- [Configuring SSH Access](#)
- [Configuring SSHD in the CSS](#)
- [Configuring Telnet Access When Using SSHD](#)
- [Showing SSHD Configurations](#)

## Enabling SSH

To enable SSH functionality in your CSS, you must purchase the Secure Management software option. If you purchased the Secure Management software option:

- During the initial CSS order placement, the software Claim Certificate is included in the accessory kit.
- After you receive the CSS, Cisco Systems sends the Claim Certificate to you by mail.



### Note

---

If you cannot locate the Secure Management option Claim Certificate in the accessory kit, call the Cisco Technical Assistance Center (TAC) toll free, 24 hours a day, 7 days a week at 1-800-553-2447 or 1-408-526-7209. You can also e-mail TAC at [tac@cisco.com](mailto:tac@cisco.com).

---

Follow the instructions on the Claim Certificate to obtain the Secure Management software license key.

To enter the Secure Management license key and activate SSH:

1. Log in to the CSS and enter the **license** command.

```
# license
```

2. Enter the Secure Management license key.

```
Enter the Software License Key (q to quit): nnnnnnnnnnnn
```

The Secure Management license key is now properly installed and the SSH function activated.

## Configuring SSH Access

SSH access to the CSS is enabled by default through the **no restrict ssh** command. You can verify the SSH access selection in the running-config file.

To enhance security when using SSHD, disable Telnet access (Telnet access is enabled by default). Use the **telnet-access disable** command as described in [Chapter 1, Controlling CSS Access](#).

To enable SSH access to the CSS, enter:

```
(config)# no restrict ssh
```

To disable SSH access, enter:

```
(config)# restrict ssh
```

## Configuring SSHD in the CSS

The CSS provides the following commands for configuring SSHD:

- **sshd keepalive** - Enables TCP keepalive messages
- **sshd port** - Specifies the SSHD port
- **sshd server-keybits** - Sets the number of bits in the ephemeral protocol server key (SSH v1 only)

Ensure you enable SSHD access to the CSS for SSHD to accept connections from SSH clients. By default, SSH access is enabled through the **no restrict ssh** global command.

## Configuring SSHD Keepalive

The CSS supports sending TCP keepalive messages to the client as a means for the server to determine whether the SSHD connection to the client is functioning (for example, if the network has gone down or the client has become unresponsive). If you disable sending SSHD keepalives to a client, sessions may hang indefinitely on the server, which consumes system resources.

Use the **sshd keepalive** command to enable SSHD keepalive. SSHD keepalive is enabled by default.

To enable sending SSHD keepalives to the client, enter:

```
(config)# sshd keepalive
```

To disable sending SSHD keepalives, enter:

```
(config)# no sshd keepalive
```

## Configuring SSHD Port

The default port number for SSH is 22. To specify the port number to which the server listens for connections from clients, use the **sshd port** command. Enter a port number of 22 or from 512 to 65535.



### Note

---

When you configure a new sshd port, you may receive a message saying that the port is invalid or unavailable. This message can appear if the port is in use internally by the CSS. If this message occurs, enter a different port number.

---

For example, to configure port number 65530 as the SSHD port, enter:

```
(config)# sshd port 65530
```

To reset the port number to the default of 22, enter:

```
(config)# no sshd port
```

## Configuring SSHD Server-Keybits

To specify the number of bits in the ephemeral protocol server key, use the **sshd server-keybits** command. The **sshd server-keybits** command pertains only to SSH v1 connections. Enter the number of bits from 512 to 1024 (the valid range). The default is 768.

**Note**

The valid range for this command is 512 to 1024. However, to maintain backward compatibility with version 5.00, the CSS allows you to enter a value from 512 to 32768. If you enter a value greater than 1024, the CSS changes the value to the default of 768. When you reboot the CSS, the following error message appears to remind you of the valid range:

```
NETMAN-3: sshd: Bad server key size <configured value>; range 512 to 1024; defaulting to 768
```

For example, to set the number of bits in the server key to 1024, enter:

```
(config)# sshd server-keybits 1024
```

To reset the number of bits to the default of 768, enter:

```
(config)# no sshd server-keybits
```

## Configuring Telnet Access When Using SSHD

By default, Telnet access to the CSS is enabled. When you use SSHD, you can disable nonsecure Telnet access to the CSS. To enhance security when using SSHD, we recommend that you disable Telnet access. Use the global `restrict telnet` command to disable Telnet access to the CSS.

To disable Telnet access, enter:

```
(config)# restrict telnet
```

To reenable Telnet access to the CSS, enter:

```
(config)# no restrict telnet
```

# Showing SSHD Configurations

Use the **show sshd** command to display SSHD configurations. This command provides the following options:

- **show sshd config** - Displays the SSHD configuration
- **show sshd sessions** - Displays a summary of the current active SSHD server sessions. The command displays data only if an SSH client is currently configured.
- **show sshd version** - Show the current version of the SSHield package running in the CSS.

To display the SSHD configuration, enter:

```
# show sshd config
```

Table 2-1 describes the fields in the **show sshd config** command output.

**Table 2-1** Field Descriptions for the **show sshd config** Command

Field	Description
Maximum Sessions Allowed	The maximum number of concurrent SSHD sessions (five maximum).
Active Sessions	The number of currently active SSHD sessions.
Log Level	The current log level.
Listen Socket Count	The number of sockets that SSHD is currently listening on (not currently configurable, default is 1).
Listen Port	The port number that SSHD uses to listen for client connections (set by the <b>sshd port</b> command). The default is 22 (the default port for SSH). The port number is 22 or from 512 to 65535.
Listen Address	The address that SSHD uses to listen for client connections (not currently configurable; default is 0.0.0.0).
Server Key Bits	The number of bits to use when generating the SSHv1 server key. The default is 768. The range is from 512 to 1024.

**Table 2-1** *Field Descriptions for the show sshd config Command (continued)*

Field	Description
RSA Protocol (SSH1)	The status of SSHv1 access (not currently configurable; default is enabled).
Empty Passwords	Disabled. The username must always have an associated password.
Keepalive	The status of sending a TCP keepalive to the client: Enabled or Disabled. SSHD keepalive is enabled by default.
SSH2 Cipher List	A list of SSHv2 cipher suites supported for authentication, encryption, and data integrity between the client and the server.

To display the SSHD sessions, enter:

```
# show sshd sessions
```

[Table 2-2](#) describes the fields in the **show sshd sessions** command output.

**Table 2-2** *Field Descriptions for the show sshd sessions Command*

Field	Description
Session_ID	The session ID.
Conn_TID	The connection task ID of the SSHD server handling the connection (tSshConn).
Login_TID	The login task ID handling the connection (tSshCli).

**Table 2-2** *Field Descriptions for the show sshd sessions Command (continued)*

Field	Description
PTY_FD	<p>The file descriptor used by the login task to communicate with the CSS CLI.</p> <p>The PTY_FD file descriptor allows you to correlate the SSH client sessions with those sessions listed under the Line field in the <b>show lines</b> output. For example, the <b>show sshd sessions</b> output displays an SSH client session connected to PTY_FD32. If you enter the <b>show lines</b> command you see a line in the display listing sshc32 (for SSH client pty_fd32). This correlation allows you to view the login time, idle time, and the location of the client of the SSH sessions through the <b>show lines</b> command.</p>
Remote IP/ Remote Port	The remote IP and port number of the SSHD session.

To display the SSHD version, enter:

```
# show sshd version
SSHield version 1.5, SSH version OpenSSH_3.0.2p1
```