Configuring Secure Shell

The Secure Shell (SSH) feature is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. Two versions of SSH are available: SSH Version 1 and SSH Version 2. Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only. For information about SSH Version 2, see the “Secure Shell Version 2 Support” feature module.

• Finding Feature Information, page 1
• Prerequisites for Configuring SSH, page 1
• Restrictions for Configuring SSH, page 2
• Information About Secure Shell (SSH), page 2
• How to Configure SSH, page 4
• Configuration Examples for SSH, page 6
• Additional References, page 11
• Feature Information for Configuring Secure Shell, page 12

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring SSH

Note

Unless otherwise noted, the term "SSH" denotes “SSH Version 1” only.
• Download the required image on the device. 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.) For information about downloading a software image, see the Loading and Managing System Images Configuration Guide.

• Configure a hostname and host domain for your device by using the `hostname` and `ip domain-name` commands in global configuration mode.

• Generate a Rivest, Shamir, and Adleman (RSA) key pair for your device. This key pair automatically enables SSH and remote authentication when the `crypto key generate rsa` command is entered in global configuration mode.

To delete the RSA key pair, use the `crypto key zeroize rsa` global configuration command. Once you delete the RSA key pair, you automatically disable the SSH server.

• Configure user authentication for local or remote access. You can configure authentication with or without authentication, authorization, and accounting (AAA). For more information, see the Authentication, Authorization, and Accounting Configuration Guide.

Restrictions for Configuring SSH

Note

Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

• The Secure Shell (SSH) server and SSH client are supported on Data Encryption Standard (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.

• Execution shell is the only application supported.

• The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.

Information About Secure Shell (SSH)

Note

Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.
SSH Server

Note

Unless otherwise noted, the term "SSH" denotes "SSH Version 1" only.

The Secure Shell (SSH) Server feature enables an SSH client to make a secure, encrypted connection to a Cisco device. This connection provides functionality that is similar to that of an inbound Telnet connection. Before SSH, security was limited to Telnet security. SSH allows a strong encryption to be used with the Cisco software authentication. The SSH server in Cisco software works with publicly and commercially available SSH clients.

SSH Integrated Client

Note

Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. 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 client in Cisco software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication. User authentication is performed like that in the Telnet session to the device. The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored usernames and passwords.

Note

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

RSA Authentication Support

Rivest, Shamir, and Adleman (RSA) authentication available in Secure Shell (SSH) clients is not supported on the SSH server for Cisco software by default. For more information about RSA authentication support, see the “Configuring a Router for SSH Version 2 Using RSA Pairs” section of the “Secure Shell Version 2 Support” module.
How to Configure SSH

Configuring an SSH Server

Note
Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip ssh {timeout seconds | authentication-retries integer}
4. ip ssh rekey {time time | volume volume}
5. exit
6. show ip ssh

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2            | Enters global configuration mode. |
| configure terminal | |
| Example:          | |
| Device# configure terminal | |

| Step 3            | Configures Secure Shell (SSH) control parameters. |
| ip ssh {timeout seconds | authentication-retries integer} | Note |
| Example:          | This command can also be used to establish the number of password prompts provided to the user. The number is the lower of the following two values: |
| Device(config)# ip ssh timeout 30 | • Value proposed by the client using the ssh -o numberofpasswordprompt command. |
|                    | • Value configured on the device using the ip ssh authentication-retries integer command, plus one. |
### Invoking an SSH Client

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

- Enter your password if prompted.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh -l username -vrf vrf-name ip-address</code></td>
<td>Invokes the SSH client to connect to an IP host or address in the specified virtual routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# ssh -l user1 -vrf vrf1 192.0.2.1</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Unless otherwise noted, the term "SSH" denotes "SSH Version 1" only.

Perform this task to invoke the Secure Shell (SSH) client. The SSH client runs in user EXEC mode and has no specific configuration tasks.

**SUMMARY STEPS**

1. `enable`
2. `ssh -l username -vrf vrf-name ip-address`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Configures a time-based rekey or a volume-based rekey for SSH.</td>
</tr>
<tr>
<td>`ip ssh rekey {time time</td>
<td>volume volume}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip ssh rekey time 108</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Verifies that the SSH server is enabled and displays the version and configuration data for the SSH connection.</td>
</tr>
<tr>
<td><code>show ip ssh</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# show ip ssh</code></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting Tips

Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

- If your Secure Shell (SSH) configuration commands are rejected as illegal commands, you have not successfully generated an Rivest, Shamir, and Adleman (RSA) key pair for your device. Make sure that you have specified a hostname and domain. Then use the **crypto key generate rsa** command to generate an RSA key pair and enable the SSH server.

- When configuring the RSA key pair, you might encounter the following error messages:
  - No hostname specified.
    You must configure a hostname for the device using the **hostname** global configuration command. See the “IPsec and Quality of Service” module for more information.
  - No domain specified.
    You must configure a host domain for the device using the **ip domain-name** global configuration command. See the “IPsec and Quality of Service” module for more information.

- The number of allowable SSH connections is limited to the maximum number of vlys configured for the device. Each SSH connection uses a vty resource.

- SSH uses either local security or the security protocol that is configured through AAA on your device for user authentication. When configuring Authentication, Authorization, and Accounting (AAA), you must ensure that AAA is disabled on the console for user authentication. AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the **no aaa authorization console** command during the AAA configuration stage.

Configuration Examples for SSH

Example SSH on a Cisco 7200 Series Router

In the following example, SSH is configured on a Cisco 7200 with a timeout that is not to exceed 60 seconds and no more than 2 authentication retries. Before the SSH server feature is configured on the router, TACACS+ is specified as the method of authentication.

```
hostname Router72K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password password
username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip domain-lookup
```
Example SSH on a Cisco 7500 Series Router

In the following example, SSH is configured on a Cisco 7500 with a timeout that is not to exceed 60 seconds and no more than 5 authentication retries. Before the SSH server feature is configured on the router, RADIUS is specified as the method of authentication.

hostname Router75K
aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com

! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 5
controller E1 3/0
  channel-group 0 timeslots 1
controller E1 3/1
  channel-group 0 timeslots 1
  channel-group 1 timeslots 2
interface Ethernet0/0/0
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  shutdown
interface Ethernet0/0/1
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  shutdown
interface Ethernet0/0/2
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  shutdown
interface Ethernet0/0/3
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  shutdown
interface Ethernet1/0
  ip address 192.168.110.2 255.255.255.0 secondary
  ip address 192.168.109.2 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
interface Ethernet1/1
  ip address 192.168.109.2 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
interface Ethernet1/2
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
interface Ethernet1/3
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
interface Ethernet1/4
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
interface Ethernet1/5
  no ip address
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
  shutdown
interface Serial2/0
  ip address 10.1.1.2 255.0.0.0
  no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
ip classless
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1
tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco
line con 0
eexec-timeout 0 0
login authentication aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4
end

Example SSH on a Cisco 12000 Series Router

In the following example, SSH is configured on a Cisco 12000 with a timeout that is not to exceed 60 seconds and no more than two authentication retries. Before the SSH server feature is configured on the router, TACACS+ is specified as the method of authentication.

hostname Router12K
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaaa12000kw local
enable password password
username username1 password 0 password1
username username2 password 0 password2
redundancy
main-cpu
auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2
interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable
interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32
interface POS1/2
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast
router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
eexec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end

Example: Verifying SSH

Note

Unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

To verify that the Secure Shell (SSH) server is enabled and to display the version and configuration data for your SSH connection, use the show ip ssh command. The following example shows that SSH is enabled:

Device# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3

The following example shows that SSH is disabled:

Device# show ip ssh
To verify the status of your SSH server connections, use the `show ssh` command. The following example shows the SSH server connections on the device when SSH is enabled:

```
Device# show ssh
Connection Version Encryption State Username
 0 1.5 3DES Session Started guest
```

The following example shows that SSH is disabled:

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

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Authentication, authorization, and accounting (AAA)</td>
<td>Authentication, Authorization, and Accounting Configuration Guide</td>
</tr>
<tr>
<td>IPsec</td>
<td>“IPsec and Quality of Service” module</td>
</tr>
<tr>
<td>SSH Version 2</td>
<td>“Secure Shell Version 2 Support” module</td>
</tr>
<tr>
<td>Downloading a software image</td>
<td>Loading and Managing System Images Configuration Guide</td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Configuring Secure Shell

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Secure Shell

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Secure Shell   | Cisco IOS 12.0(5)S  
Cisco IOS 15.1(1)SY | The Secure Shell (SSH) feature is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. Two versions of SSH are available: SSH Version 1 and SSH Version 2. This document describes SSH Version 1. This document also includes information about the Secure Shell SSH Version 1 Integrated Client feature and the Secure Shell SSH Version 1 Server Support feature. Both features are part of the Secure Shell functionality. |