



Configuring Secure Shell (SSH)

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Configuring the Switch for Secure Shell \(SSH\) and Secure Copy Protocol \(SCP\), on page 1](#)
- [Restrictions for Configuring the Switch for SSH, on page 2](#)
- [Information about SSH, on page 2](#)
- [How to Configure SSH, on page 4](#)
- [Monitoring the SSH Configuration and Status, on page 8](#)
- [Additional References for Configuring Secure Shell, on page 8](#)
- [Feature Information for SSH, on page 9](#)

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 <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Prerequisites for Configuring the Switch for Secure Shell (SSH) and Secure Copy Protocol (SCP)

The following are the prerequisites for configuring the switch for secure shell (SSH):

- To use SSH, you must install the cryptographic (encrypted) software image on your switch.
- For SSH to work, the switch needs an 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.

Related Topics

[Secure Copy Protocol](#), on page 4

Restrictions for Configuring the Switch for SSH

The following are restrictions for configuring the Switch for secure shell.

- 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 DES (56-bit) and 3DES (168-bit) data encryption software.
- The Switch 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.
- This software release does not support IP Security (IPSec).
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.

Related Topics

[Secure Copy Protocol](#), on page 4

Information about SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Switch Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

Related Topics

[Configuring the Switch for Local Authentication and Authorization](#)

[TACACS+ and Switch Access](#)

[RADIUS and Switch Access](#)

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.

Related Topics

[Setting Up the Switch to Run SSH](#), on page 4

[Configuring the Switch for Local Authentication and Authorization](#)

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/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 an 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

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. The behavior of SCP is similar to that of remote copy (rtp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the switch can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

Related Topics

[Prerequisites for Configuring the Switch for Secure Shell \(SSH\) and Secure Copy Protocol \(SCP\)](#), on page 1

[Restrictions for Configuring the Switch for SSH](#), on page 2

How to Configure SSH

Setting Up the Switch to Run SSH

Follow these steps to set up your Switch to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *domain_name*
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Switch> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	hostname <i>hostname</i> Example: <pre>Switch(config)# hostname your_hostname</pre>	Configures a hostname and IP domain name for your Switch. Note Follow this procedure only if you are configuring the Switch as an SSH server.
Step 4	ip domain-name <i>domain_name</i> Example: <pre>Switch(config)# ip domain-name your_domain</pre>	Configures a host domain for your Switch.
Step 5	crypto key generate rsa Example: <pre>Switch(config)# crypto key generate rsa</pre>	Enables the SSH server for local and remote authentication on the Switch and generates an RSA key pair. Generating an RSA key pair for the Switch 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 Switch as an SSH server.
Step 6	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Switch(config)# end	
Step 7	show running-config Example: Switch# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[SSH Configuration Guidelines](#), on page 3

[Configuring the Switch for Local Authentication and Authorization](#)

Configuring the SSH Server

Follow these steps to configure the SSH server:



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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh version [1 | 2]**
4. **ip ssh {time-out *seconds* | authentication-retries *number*}**
5. Use one or both of the following:
 - **line vtyline_number[ending_line_number]**
 - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>ip ssh version [1 2]</p> <p>Example:</p> <pre>Switch(config)# ip ssh version 1</pre>	<p>(Optional) Configures the Switch to run SSH Version 1 or SSH Version 2.</p> <ul style="list-style-type: none"> • 1—Configure the Switch to run SSH Version 1. • 2—Configure the Switch to run SSH Version 2. <p>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. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.</p>
Step 4	<p>ip ssh {time-out <i>seconds</i> authentication-retries <i>number</i>}</p> <p>Example:</p> <pre>Switch(config)# ip ssh time-out 90 OR Switch(config)# ip ssh authentication-retries 2</pre>	<p>Configures the SSH control parameters:</p> <ul style="list-style-type: none"> • time-out <i>seconds</i>: 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. After the connection is established, the Switch uses the default time-out values of the CLI-based sessions. • authentication-retries <i>number</i>: Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. <p>Repeat this step when configuring both parameters.</p>
Step 5	<p>Use one or both of the following:</p> <ul style="list-style-type: none"> • line <i>vt</i><i>line_number</i>[<i>ending_line_number</i>] • transport input ssh <p>Example:</p> <pre>Switch(config)# line vty 1 10</pre> <p>or</p>	<p>(Optional) Configures the virtual terminal line settings.</p> <ul style="list-style-type: none"> • Enters line configuration mode to configure the virtual terminal line settings. For <i>line_number</i> and <i>ending_line_number</i>, specify a pair of lines. The range is 0 to 15. • Specifies that the Switch prevent non-SSH Telnet connections. This limits the router to only SSH connections.

	Command or Action	Purpose
	Switch(config-line) # <code>transport input ssh</code>	
Step 6	end Example: Switch(config-line) # <code>end</code>	Returns to privileged EXEC mode.
Step 7	show running-config Example: Switch# <code>show running-config</code>	Verifies your entries.
Step 8	copy running-config startup-config Example: Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 1: Commands for Displaying the SSH Server Configuration and Status

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

Additional References for Configuring Secure Shell

Related Documents

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for SSH

Release	Feature Information
Cisco IOS Release 15.0(2)EX	This feature was introduced.

