



Secure Copy

This document provides the procedure to configure a Cisco device for Secure Copy (SCP) server-side functionality.

- [Prerequisites for Secure Copy, on page 1](#)
- [Information About Secure Copy, on page 1](#)
- [How to Configure Secure Copy, on page 2](#)
- [How to Configure Secure Copy, on page 5](#)
- [Additional References for Secure Copy, on page 5](#)
- [Feature History for Secure Copy, on page 6](#)

Prerequisites for Secure Copy

- Configure Secure Shell (SSH), authentication, and authorization on the device.
- Because SCP relies on SSH for its secure transport, the device must have a Rivest, Shamir, and Adelman (RSA) key pair.

Information About Secure Copy

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

The behavior of SCP is similar to that of Remote Copy Protocol (RCP), which comes from the Berkeley r-tools suite (Berkeley university's own set of networking applications), except that SCP relies on SSH for security. In addition, SCP requires authentication, authorization, and accounting (AAA) to be configured to ensure that the device can determine whether a user has the correct privilege level.

SCP allows only users with a privilege level of 15 to copy a file in the Cisco IOS File System (Cisco IFS) to and from a device by using the **copy** command. An authorized administrator can also perform this action from a workstation.



- Note**
- Enable the SCP option while using the `pscp.exe` file.
 - An RSA public-private key pair must be configured on the device for SSH to work.

Similar to SCP, SSH File Transfer Protocol (SFTP) can be used to copy switch configuration or image files. For more information, refer the *Configuring SSH File Transfer Protocol* chapter of the *Security Configuration Guide*.

How to Configure Secure Copy

Configuring Secure Copy

To configure a Cisco device for SCP server-side functionality, perform the following steps.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Sets AAA authentication at login. |
| Step 4 | aaa authentication login {default list-name} method1 [method2...] Example: Device(config)# aaa authentication login default group tacacs+ | Enables the AAA access control system. |
| Step 5 | username name [privilege level] password encryption-type encrypted-password Example: | Establishes a username-based authentication system. |

| | Command or Action | Purpose |
|---------------|---|---|
| | <pre>Device(config)# username superuser privilege 2 password 0 superpassword</pre> | Note You can omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured. |
| Step 6 | ip scp server enable Example: <pre>Device(config)# ip scp server enable</pre> | Enables SCP server-side functionality. |
| Step 7 | exit Example: <pre>Device(config)# exit</pre> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 8 | debug ip scp Example: <pre>Device# debug ip scp</pre> | (Optional) Troubleshoots SCP authentication problems. |

Enabling Secure Copy Protocol on the SSH Server

The following task shows how to configure the server-side functionality for SCP. This task shows a typical configuration that allows a device to securely copy files from a remote workstation.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. Enter your password, if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | aaa new-model Example: <pre>Device(config)# aaa new-model</pre> | Enables the Authentication, Authorization, and Accounting (AAA) access control model. |
| Step 4 | aaa authentication login default local Example: | Sets AAA authentication to use the local username database for authentication at login. |

| | Command or Action | Purpose |
|----------------|--|--|
| | Device (config) # <code>aaa authentication login default local</code> | |
| Step 5 | aaa authorization exec default local Example: Device (config) # <code>aaa authorization exec default local</code> | Sets the parameters that restrict user access to a network, runs the authorization to determine if the user ID is allowed to run an EXEC shell, and specifies that the system must use the local database for authorization. |
| Step 6 | username <i>name</i> privilege <i>privilege-level</i> password <i>password</i> Example: Device (config) # <code>username samplename privilege 15 password password1</code> | Establishes a username-based authentication system, and specifies the username, privilege level, and an unencrypted password. Note The minimum value for the <i>privilege-level</i> argument is 15. A privilege level of less than 15 results in the connection closing. |
| Step 7 | ip ssh time-out <i>seconds</i> Example: Device (config) # <code>ip ssh time-out 120</code> | Sets the time interval (in seconds) that the device waits for the SSH client to respond. |
| Step 8 | ip ssh authentication-retries <i>integer</i> Example: Device (config) # <code>ip ssh authentication-retries 3</code> | Sets the number of authentication attempts after which the interface is reset. |
| Step 9 | ip scp server enable Example: Device (config) # <code>ip scp server enable</code> | Enables the device to securely copy files from a remote workstation. |
| Step 10 | ip ssh bulk-mode Example: Device (config) # <code>ip ssh bulk-mode</code> | (Optional) Enables SSH bulk data transfer mode to enhance the throughput performance of SCP. |
| Step 11 | exit Example: Device (config) # <code>exit</code> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 12 | debug ip scp Example: Device# <code>debug ip scp</code> | (Optional) Provides diagnostic information about SCP authentication problems. |

How to Configure Secure Copy

Example: Secure Copy Configuration Using Local Authentication

The following example shows how to configure the server-side functionality of SCP. This example uses a locally defined username and password.

```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end
```

Example: SCP Server-Side Configuration Using Network-Based Authentication

The following example shows how to configure the server-side functionality of SCP using a network-based authentication mechanism:

```
! AAA authentication and authorization must be configured properly for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group tacacs+
Device(config)# aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
Device(config)# ip ssh time-out 120
Device(config)# ip ssh authentication-retries 3
Device(config)# ip scp server enable
Device(config)# end
```

Additional References for Secure Copy

Related Documents

| Related Topic | Document Title |
|--------------------------------------|---------------------------------|
| Secure Shell Version 1 and 2 support | <i>Configuring Secure Shell</i> |

Technical Assistance

| Description | Link |
|---|---|
| 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. | http://www.cisco.com/cisco/web/support/index.html |

Feature History for Secure Copy

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|------------------------------|-------------|---|
| Cisco IOS XE Everest 16.5.1a | Secure Copy | <p>The Secure Copy feature provides a secure and authenticated method for copying device configurations or device image files. SCP relies on SSH, an application and protocol that provide a secure replacement for the Berkeley r-tools suite.</p> <p>The following commands were introduced or modified: debug ip scp and ip scp server enable.</p> |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.