



Secure Copy

The Secure Copy (SCP) feature provides a secure and authenticated method for copying device configurations or device image files. SCP relies on Secure Shell (SSH), an application and protocol that provide a secure replacement for the Berkeley r-tools suite (Berkeley university's own set of networking applications). This document provides the procedure to configure a Cisco device for SCP server-side functionality.

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Secure Copy, on page 1](#)
- [Information About Secure Copy, on page 2](#)
- [How to Configure Secure Copy, on page 2](#)
- [Configuration Examples for Secure Copy, on page 4](#)
- [Additional References, on page 4](#)
- [Glossary, on page 5](#)

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfng.cisco.com/>. An account on Cisco.com is not required.

Prerequisites for Secure Copy

- Before enabling Secure Copy (SCP), you must correctly 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

How Secure Copy Works

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

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



Note Enable the SCP option while using the pscp.exe file with the Cisco software.

The Cisco router running on IOS XE considers 1024 bytes * 32 blocks (32768 bytes) per TCP window size. A bad length error message is displayed for packets that flow in beyond this parameter.

How to Configure Secure Copy

Configuring Secure Copy

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

Procedure

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:

```
Device(config)# username superuser privilege 2 password 0 superpassword
```

Establishes a username-based authentication system.

Note You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.

Step 6 **ip scp server enable**

Example:

```
Device(config)# ip scp server enable
```

Enables SCP server-side functionality.

Step 7 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 8 **show running-config**

Example:

```
Device# show running-config
```

(Optional) Displays the SCP server-side functionality.

Step 9 **debug ip scp**

Example:

```
Device# debug ip scp
```

(Optional) Troubleshoots SCP authentication problems.

Configuration Examples for Secure Copy

Example: Secure Copy Configuration Using Local Authentication

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

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

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.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Secure Shell Version 1 and 2 support	<i>Secure Shell Configuration Guide</i>
Authentication and authorization commands	Cisco IOS Security Command Reference: Commands A to C
Configuring authentication and authorization	<i>Authentication, Authorization, and Accounting Configuration Guide</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

Glossary

AAA—authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

RCP—remote copy. Relies on Remote Shell (Berkeley r-tools suite) for security; RCP copies files such as device images and startup configurations to and from devices.

SCP—secure copy. Relies on SSH for security; SCP support allows secure and authenticated copying of anything that exists in the Cisco IOS File System (IFS). SCP is derived from RCP.

SSH—Secure Shell. An application and protocol that provide a secure replacement for the Berkeley r-tools suite. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similar to the Berkeley rexec and rsh tools. SSH Version 1 is implemented in the Cisco software.

