Secure Copy

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

Prerequisites for Secure Copy

- Configure Secure Shell (SSH), authentication, and authorization on the device.
- Because the Secure Copy Protocol (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*.

Secure Copy Performance Improvements

SSH bulk data transfer mode can be used to enhance the throughput performance of SCP that is operating in the capacity of a client or a server. This mode is disabled by default, but can be enabled by using the **ip ssh bulk-mode** global configuration command. TCP selective acknowledgement (SACK) is enabled by default if the bulk mode window size is configured.

Note We recommend that you enable this command only for transferring large files, and disable it after the file transfer is complete.

The default bulk mode window size of 128 KB is optimal to copy large files in most network settings. However, in long big networks where the round-trip time (RTT) is high, 128 KB is not enough. You can enable the most optimal SCP throughput performance by configuring the bulk mode window size using the **ip ssh bulk-mode** *window-size* command. For example, in an ideal lab testing environment, a window size of 2 MB in a 200-milliseconds round-trip time setting can give around 500 percent improved throughput performance when compared to the default 128-KB window size.

The bulk mode window size must be configured as per the network bandwidth-delay product, that is, a multiple of total available bandwidth in bits per second and the round-trip time in seconds. Because the CPU usage may increase with the increased window size, make sure to balance this by choosing the right window size.

How to Configure Secure Copy

The following sections provide information about the Secure Copy configuration tasks.

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.

	Command or Action	Purpose
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 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:** `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	**debug ip scp** **Example:** `Device# debug ip scp`	(Optional) Troubleshoots SCP authentication problems.

Enabling Secure Copy 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:** `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`	Enables the Authentication, Authorization, and Accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	Sets AAA authentication to use the local username database for authentication at login.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network, runs the authorization to determine if the user ID is allowed to run an privileged EXEC shell, and specifies that the system must use the local database for authorization.
Step 6	**username** *name* **privilege** *privilege-level* **password** *password* **Example:** `Device(config)# username samplename privilege 15 password password1`	Establishes a username-based authentication system, and specifies the username, privilege level, and an unencrypted password. **Note** The minimum required value for the *privilege-level* argument is 15. A privilege level of less than 15 results in the connection closing.
Step 7	**ip ssh time-out** *seconds* **Example:** `Device(config)# ip ssh time-out 120`	Sets the time interval (in seconds) that the device waits for the SSH client to respond.
Step 8	**ip ssh authentication-retries** *integer* **Example:** `Device(config)# ip ssh authentication-retries 3`	Sets the number of authentication attempts after which the interface is reset.
Step 9	**ip scp server enable** **Example:** `Device(config)# ip scp server enable`	Enables the device to securely copy files from a remote workstation.

	Command or Action	Purpose
Step 10	**ip ssh bulk-mode** *window-size* **Example:** `Device(config)# ip ssh bulk-mode 33107232`	(Optional) Enables SSH bulk data transfer mode to enhance the throughput performance of SCP.
Step 11	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 12	**debug ip scp** **Example:** `Device# debug ip scp`	(Optional) Provides diagnostic information about SCP authentication problems.

Configuration Examples for Secure Copy

The following are examples of the Secure Copy configuration.

Example: Secure Copy Configuration Using Local Authentication

The following example shows how to configure the server-side functionality of Secure Copy. 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: Secure Copy Server-Side Configuration Using Network-Based Authentication

The following example shows how to configure the server-side functionality of Secure Copy 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	*Configuring Secure Shell*

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	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. The following commands were introduced or modified: **debug ip scp** and **ip scp server enable**. Support for this feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	Secure Copy	Support for this feature was introduced only on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Amsterdam 17.2.1	Secure Copy Performance Improvements	SSH bulk mode enables certain optimizations to enhance the throughput performance of procedures involving large amount of data transfer. This mode can be enabled by using the **ip ssh bulk-mode** global configuration command.
Cisco IOS XE Bengaluru 17.6.1	Secure Copy Improvement in Large RTT Scenario	Secure copy in large RTT settings can be configured by using the *window-size* variable option of the **ip ssh bulk-mode** command.
Cisco IOS XE Cupertino 17.7.1	Secure Copy	Support for this feature was introduced on the C9500X-28C8D model of the Cisco Catalyst 9500 Series Switches.

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.