# Secure Copy

**Last Updated: July 04, 2011**

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


- Finding Feature Information, page 1
- Prerequisites for Secure Copy, page 1
- Information About Secure Copy, page 2
- How to Configure Secure Copy, page 2
- Configuration Examples for Secure Copy, page 4
- Additional References, page 5
- Feature Information for Secure Copy, page 6
- Glossary, page 7


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Secure Copy

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.

- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

# Information About Secure Copy

- How Secure Copy Works, page 2

## How Secure Copy Works

The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the **copy** command. An authorized administrator may also perform this action from a workstation.

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

# How to Configure Secure Copy

- Configuring Secure Copy, page 2

## Configuring Secure Copy

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1*[*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
6. **username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*}
7. **ip scp server enable**
8. **show running-config**
9. **debug ip scp**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Sets AAA authentication at login. |
| **Step 4** | **aaa authentication login** {**default** \| *list-name*} *method1*[*method2*...]<br><br>**Example:**<br>`Router(config)# aaa authentication login default group tacacs+` | Enables the AAA access control system. |
| **Step 5** | **aaa authorization** {**network** \| **exec** \| **commands** *level* \| **reverse-access** \| **configuration**} {**default** \| *list-name*} [*method1* [*method2*...]]<br><br>**Example:**<br>`Router(config)# aaa authorization exec default group tacacs+` | Sets parameters that restrict user access to a network.<br>**Note** **The exec** keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use it when you configure SCP. |
| **Step 6** | **username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*}<br><br>**Example:**<br>`Router(config)# username superuser privilege 2 password 0 superpassword` | Establishes a username-based authentication system.<br>**Note** You may omit this step if a network-based authentication mechanism--such as TACACS+ or RADIUS--has been configured. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **ip scp server enable**<br><br>**Example:**<br>`Router(config)# ip scp server enable` | Enables SCP server-side functionality. |
| **Step 8** | **show running-config**<br><br>**Example:**<br>`Router# show running-config` | (Optional) Verifies the SCP server-side functionality. |
| **Step 9** | **debug ip scp**<br><br>**Example:**<br>`Router# debug ip scp` | (Optional) Troubleshoots SCP authentication problems. |

# Configuration Examples for Secure Copy


- Example SCP Server-Side Configuration Using Local Authentication, page 4
- Example SCP Server-Side Configuration Using Network-Based Authentication, page 4


## Example SCP Server-Side 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 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 ssh time-out 120
ip ssh authentication-retries 3
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 Commands List, All Releases |
| Secure Shell Version 1 and 2 support | • Configuring Secure Shell module<br>• Secure Shell Version 2 Support module |
| Authentication and authorization commands | Cisco IOS Security Command Reference |
| Configuring authentication and authorization | Authentication, Authorization, and Accounting (AAA) section of *Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0 |

### Standards

| Standards | Title |
|---|---|
| None | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| None | -- |

### 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 Information for Secure Copy

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 Secure Copy***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Secure Copy | 12.2(2)T 12.0(21)S 12.2(25)S | The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provide a secure replacement for the Berkeley r-tools.<br>This feature was introduced in Cisco IOS Release 12.2(2)T.<br>This feature was integrated into Cisco IOS Release 12.0(21)S.<br>This feature was integrated into Cisco IOS Release 12.2(25)S.<br>The following commands were introduced or modified: **debug ip scp, ip scp server enable**. |

# Glossary

**AAA** --authentication, authorization, and accounting. 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. Relying on Remote Shell (Berkeley r-tools suite) for security, rcp copies files, such as router images and startup configurations, to and from routers.

**SCP** --secure copy. Relying on SSH for security, SCP support allows the secure and authenticated copying of anything that exists in the Cisco IOS File System. SCP is derived from rcp.

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