



## Secure Copy

---

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.

### Feature History for Secure Copy

Release	Modification
12.2(2)T	This feature was introduced.
12.0(21)S	This feature was integrated into Cisco IOS 12.0(21)S.
12.2(25)S	This feature was integrated into Cisco IOS 12.2(25)S.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Secure Copy, page 2](#)
- [Information About Secure Copy, page 2](#)
- [How to Configure SCP, page 2](#)
- [Configuration Examples for Secure Copy, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 10](#)



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

## 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

To configure Secure Copy feature, you should understand the following concepts.

- [How SCP Works, page 2](#)

## How SCP 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.

## How to Configure SCP

This section contains the following procedures:

- [Configuring SCP, page 2](#)
- [Verifying SCP, page 4](#)
- [Troubleshooting SCP, page 4](#)

## Configuring SCP

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**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router (config)# aaa new-model	Sets AAA authentication at login.
Step 4	<b>aaa authentication login</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]  <b>Example:</b> Router (config)# aaa authentication login default group tacacs+	Enables the AAA access control system.
Step 5	<b>aaa authorization</b> { <b>network</b>   <b>exec</b>   <b>commands</b> <i>level</i>   <b>reverse-access</b>   <b>configuration</b> } { <b>default</b>   <i>list-name</i> } [ <i>method1</i> [ <i>method2...</i> ]]  <b>Example:</b> Router (config)# aaa authorization exec default group tacacs+	Sets parameters that restrict user access to a network.  <b>Note</b> The <b>exec</b> 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	<b>username</b> <i>name</i> [ <b>privilege level</b> ] { <b>password</b> <i>encryption-type encrypted-password</i> }  <b>Example:</b> Router (config)# username superuser privilege 2 password 0 superpassword	Establishes a username-based authentication system.  <b>Note</b> You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has been configured.
Step 7	<b>ip scp server enable</b>  <b>Example:</b> Router (config)# ip scp server enable	Enables SCP server-side functionality.

## Verifying SCP

To verify SCP server-side functionality, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `show running-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Verifies the SCP server-side functionality.

## Troubleshooting SCP

To troubleshoot SCP authentication problems, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `debug ip scp`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug ip scp</b>  <b>Example:</b> Router# debug ip scp	Troubleshoots SCP authentication problems.

# Configuration Examples for Secure Copy

This section provides the following configuration examples:

- [SCP Server-Side Configuration Using Local Authentication: Example, page 5](#)
- [SCP Server-Side Configuration Using Network-Based Authentication: Example, page 5](#)

## SCP Server-Side Configuration Using Local Authentication: Example

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 tiger 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
```

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

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

The following sections provide references related to Secure Copy.

## Related Documents

Related Topic	Document Title
Secure Shell	<ul style="list-style-type: none"> <li>• <a href="#">Secure Shell Version 1 Support</a></li> <li>• <a href="#">Secure Shell Version 2 Support</a></li> </ul>
Authentication and authorization commands	<a href="#">Cisco IOS Security Command Reference</a> , Release 12.3 T
Configuring authentication and authorization	“ <a href="#">Authentication, Authorization, and Accounting (AAA)</a> ” section of <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.3

## Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents only new commands.

- [debug ip scp](#)
- [ip scp server enable](#)

# debug ip scp

To troubleshoot secure copy (SCP) authentication problems, use the **debug ip scp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip scp**

**no debug ip scp**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

**Examples** The following example is sample output from the **debug ip scp** command. In this example, a copy of the file `scptest.cfg` from a UNIX host running configuration of the router was successful.

```
Router# debug ip scp

4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv C0644 20 scptest.cfg
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv 20 bytes
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <OK>
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <EOF>
```

The following example is also sample output from the **debug ip scp** command, but in this example, the user has privilege 0 and is therefore denied:

```
Router# debug ip scp

4d06h:SCP:[22 -> 10.11.29.252:1018] send Privilege denied.
```

Related Commands	Command	Description
	<a href="#">ip scp server enable</a>	Enables SCP server-side functionality.

# ip scp server enable

To enable secure copy (SCP) server-side functionality, use the **ip scp server enable** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip scp server enable**

**no ip scp server enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled.

**Command Modes** Global configuration

## Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

## Usage Guidelines

Use the **ip scp server enable** command to enable a Cisco router to support SCP server-side functionality, which allows an authenticated user to securely copy configuration and image files to or from a remote workstation.

Before a user can utilize the SCP server-side functionality, Secure Shell (SSH), authentication, and authorization must be properly configured so a router can determine whether a user is at the correct privilege level.

## Examples

The following example shows how to transfer a file from the router using SCP:

```
Router# copy flash:c3620-ik9s-mz.122-0.17.T scp://tiger@10.1.1.2/
Address or name of remote host [10.1.1.2]?
Destination username [tiger]?
Destination filename [c3620-ik9s-mz.122-0.17.T]?
Writing c3620-ik9s-mz.122-0.17.T
Password:
```

```
Router#
```



### Note

When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa authentication login</b>	Sets AAA authentication at login.
<b>aaa authorization</b>	Sets parameters that restrict user access to a network.
<b>copy</b>	Copies any file from a source to a destination.
<b>username</b>	Establishes a username-based authentication system.

# 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 Systems. 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.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 – 2004 Cisco Systems, Inc. All rights reserved.