



ip inspect through ip security strip

- [ip scp server enable, page 2](#)

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), 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.

Command Default The secure copy function is 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 and support for the Cisco 7500 series and Cisco 12000 series routers was added.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(15)S.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines Use this command to enable secure copying of files from systems using the Secure Shell (SSH) application. This secure copy function is accomplished by an addition to the **copy** command in the Cisco IOS software, which takes care of using the secure copy protocol (scp) to copy to and from a router while logged in to the router itself. Because copying files is generally a restricted operation in the Cisco IOS software, a user attempting to copy such files needs to be at the correct enable level.

The Cisco IOS software must also allow files to be copied to or from itself from a remote workstation running the SSH application (which is supported by both the Microsoft Windows and UNIX operating systems). To get this information, the Cisco IOS software must have authentication and authorization configured in the authentication, authorization, and accounting (AAA) feature. SSH already relies on AAA authentication to authenticate the user username and password. Scp adds the requirement that AAA authorization be turned on so that the operating system can determine whether or not the user is at the correct privilege level.

Examples

The following example shows a typical configuration that allows the router to securely copy files from a remote workstation. Because scp relies on AAA authentication and authorization to function properly, AAA must be configured.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
username user1 privilege 15 password 0 lab
ip scp server enable
```

The following example shows how to use scp to copy a system image from Flash memory to a server that supports SSH:

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/
Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```



Note

When using scp, you cannot enter the password into the **copy** command; enter the password when prompted.

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
copy	Copies any file from a source to a destination.
debug ip scp	Troubleshoots scp authentication problems.
ip ssh port	Enables secure network access to the tty lines.
username	Establishes a username-based authentication system.

