



CHAPTER 13

Performing Maintenance Tasks

This chapter describes how to perform tasks used for general care and maintenance of the Cisco Guard (Guard) and contains the following sections:

- [Configuring File Servers](#)
- [Exporting the Configuration](#)
- [Importing and Updating the Configuration](#)
- [Exporting Files Automatically](#)
- [Reloading the Guard](#)
- [Rebooting the Guard and Inactivating Zones](#)
- [Shutting Down the Guard](#)
- [Upgrading the Guard Software Version](#)
- [Burning a New Flash Version to Upgrade the Common Firmware Environment](#)
- [Resetting the Linux root or Guard admin User Account Password](#)
- [Resetting the Guard Configuration to Factory Defaults](#)

Configuring File Servers

You can define a network server on the Guard for importing and exporting files between the Guard and the server. The Guard allows you to create a network server profile in which you define the network server attributes such as the IP address, the communication method, and the login details. Creating a network server profile allows you to specify just the server name when importing or exporting files.

After you configure the network server, you must configure the export or the import commands. For example, use the **export reports** commands to configure the Guard to export attack reports to a network server.

To configure a network server, use one of the following commands in configuration mode:

- **file-server** *file-server-name description ftp server remote-path login password*
- **file-server** *file-server-name description [sftp | scp] server remote-path login*

Table 13-1 provides the arguments and keywords for the **file-server** command.

Table 13-1 Arguments and Keywords for the file-server Command

Parameter	Description
<i>file-server-name</i>	Name for the network server. Enter an alphanumeric string from 1 to 63 characters. The string can contain underscores but cannot contain any spaces.
<i>description</i>	String to describe the network server. The maximum alphanumeric string length is 80 characters. If you use spaces in the expression, enclose the expression in quotation marks (“ ”).
ftp	Specifies File Transport Protocol (FTP).
sftp	Specifies Secure File Transport Protocol (SFTP).
scp	Specifies Secure Copy Protocol (SCP).
<i>server</i>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
<i>remote-path</i>	Complete path of the directory in which to save the files or from which to import the files.
<i>login</i>	Login name for the network server.
<i>password</i>	Password for the network server. This option is valid only for an FTP server. The Guard authenticates network servers that use SFTP and SCP using a public key.



Note

Because SFTP and SCP rely on Secure Shell (SSH) for secure communication, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the “[Configuring the Keys for SFTP and SCP Connections](#)” section on page 3-25 for more information.

The following example shows how to define an FTP server with the IP address 10.0.0.191:

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP server" ftp 10.0.0.191
/root/ConfigFiles <user> <password>
```

To delete a network server, use the **no file-server** [*file-server-name* | *] command in configuration mode.

To display the list of network servers, use the **show file-servers** command in global or configuration mode.

Exporting the Configuration

You can export the Guard configuration file or a zone configuration file (running-config) to a network server, which allows you to do the following:

- Implement the Guard configuration parameters on another Guard
- Back up the Guard configuration

To export the Guard configuration file, use one of the following commands in global mode:

- **copy** [zone *zone-name*] **running-config ftp** *server full-file-name* [*login* [*password*]]
- **copy** [zone *zone-name*] **running-config {sftp | scp}** *server full-file-name login*

- `copy [zone zone-name] running-config file-server-name dest-file-name`

Table 13-2 provides the arguments and keywords for the `copy running-config ftp` command.

Table 13-2 Arguments and Keywords for the `copy running-config ftp` Command

Parameter	Description
<code>zone zone-name</code>	(Optional) Specifies the zone name. If you specify the zone name, the Guard exports the zone configuration file. The default is to export the Guard configuration file.
<code>running-config</code>	Exports the complete Guard configuration or the configuration of the specified zone.
<code>ftp</code>	Specifies FTP.
<code>sftp</code>	Specifies SFTP.
<code>scp</code>	Specifies SCP.
<code>server</code>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
<code>full-file-name</code>	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
<code>login</code>	(Optional) Server login name. The <code>login</code> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
<code>password</code>	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.
<code>file-server-name</code>	Name of a network server to which to export the configuration file. You must configure the network server using the <code>file-server</code> command (see the “Configuring File Servers” section on page 13-1).
<code>dest-file-name</code>	Name of the configuration file on the remote server. The Guard saves the configuration file on the network server using the destination filename in the directory that you defined for the network server by using the <code>file-server</code> command.



Note

If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. If you do not configure the key that the Guard uses before you enter the `copy` command with the `sftp` or `scp` option, the Guard prompts you for the password. See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-25 for more information.

The following example shows how to export the Guard configuration file to an FTP server:

```
user@GUARD# copy running-config ftp 10.0.0.191 run-conf.txt <user> <password>
```

The following example shows how to export the Guard configuration file to a network server:

```
user@GUARD# copy running-config CorpFTP Configuration-12-11-05
```

Importing and Updating the Configuration

You can import a Guard or zone configuration file from an FTP server and reconfigure the Guard according to the newly transferred file. Import the configuration to do one of the following tasks:

- Configure the Guard based on an existing Guard configuration file
- Restore the Guard configuration

Zone configuration is a partial Guard configuration. To copy both types of configuration files to the Guard and reconfigure it accordingly, use the **copy ftp running-config** command.



Note

The new configuration replaces the existing configuration. You must reload the Guard for the new configuration to take effect.

We recommend that you deactivate all zones before you initiate the import process. The Guard deactivates a zone before importing the zone configuration.

The Guard, by default, ignores older versions of the self-protection configuration. We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current version.

To import a Guard configuration file, use one of the following commands in global mode:

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy** {*sftp* | *scp*} **running-config** *server full-file-name login*
- **copy** *file-server-name* **running-config** *source-file-name*

Table 13-3 provides the arguments for the **copy ftp running-config** command.

Table 13-3 Arguments for the copy ftp running-config Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
<i>server</i>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
<i>full-file-name</i>	Complete name of the file. If you do not specify a path, the server searches for the file in your home directory.
<i>login</i>	(Optional) Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
<i>password</i>	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.
<i>file-server-name</i>	Name of a network server. You must configure the network server using the file-server command (see the “Configuring File Servers” section on page 13-1).
<i>source-file-name</i>	Name of the file to import. The Guard appends the name of the file to the path that you defined for the network server by using the file-server command.

**Note**

If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. If you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the “[Configuring the Keys for SFTP and SCP Connections](#)” section on page 3-25 for more information.

The following example shows how to import the Guard configuration file from an FTP server:

```
user@GUARD# copy ftp running-config 10.0.0.191 /root/backup/conf/scannet-conf <user>
<password>
```

The following example shows how to import the Guard configuration file from a network server:

```
user@GUARD# copy CorpFTP running-config scannet-conf
```

When you import a configuration that was exported from an older version, the Guard displays the following message:

```
WARNING: The configuration file includes a self-protection definition that is incompatible
with the current version and will be ignored.
Continue? [yes|no]
```

Enter one of the following options:

- **yes**—Ignores the old self-protection configuration. The Guard performs as follows:
 - Ignores the old self-protection configuration and does not import it
 - Imports all other configurations, such as the zone, interface, and services configuration
- **no**—Enables you to import the old self-protection configuration. The Guard displays the following message:

```
You can abort the import process or import the old self-protection definition as-is.
WARNING: The self-protection definitions are incompatible with the current version.
Abort? [yes|no]
```

**Caution**

We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current software version.

To import the older self-protection configuration, enter **no**.

To abort the import process, enter **yes**.

Exporting Files Automatically

You can configure the Guard to export the following file to a network server automatically:

- Packet-dump capture files—The Guard exports the packet-dump capture files when the capture buffer size reaches 50 MB or after 10 minutes have elapsed. See the “[Exporting Packet-Dump Capture Files Automatically](#)” section on page 12-14 for more information.
- Attack reports—The Guard exports the reports of any one of the zones when an attack on the zone ends. See the “[Exporting Attack Reports Automatically](#)” section on page 11-12 for more information.

The Guard exports the packet-dump capture files and the attack reports in Extensible Markup Language (XML) format. The software version is accompanied by xsd files that describe the XML schema. You can download the xsd files from www.cisco.com.

To export files automatically to a network server, perform the following steps:

- Step 1** Define the network server to which you can export files.
See the “[Configuring File Servers](#)” section on page 13-1 for more information.
- Step 2** Configure the Guard to export files automatically by entering the following command:

```
export {packet-dump | reports} file-server-name
```

Table 13-4 provides the arguments and keywords for the **export** command.

Table 13-4 Arguments and Keywords for the export Command

Parameter	Description
packet-dump	Exports packet-dump capture files each time that the contents of the packet-dump buffer are saved to a local file. The Guard exports the packet-dump capture files in PCAP format, which is compressed and encoded by the gzip (GNU zip) program, with an accompanying file in XML that describes the recorded data. See the Capture.xsd file that accompanies the version for a description of the XML schema. See the “ Monitoring Network Traffic and Extracting Attack Signatures ” section on page 12-9 for more information about packet-dump capture files.
reports	Exports attack reports in XML format at the end of an attack. The Guard exports the reports of any one of the zones when an attack on the zone ends. See the ExportedReports.xsd file that accompanies the version for a description of the XML schema. See the “ Exporting Attack Reports ” section on page 11-11 for more information.
<i>file-server-name</i>	Name of the network server on which you can save files. You must configure the network server using the file-server command (see the “ Configuring File Servers ” section on page 13-1).

The following example shows how to define an FTP server with the IP address 10.0.0.191 and then to configure the Guard to automatically export reports (in XML) at the end of an attack to that server:

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP server" ftp 10.0.0.191  
/root/ConfigFiles <user> <password>  
user@GUARD-conf# export reports CorpFTP-Server
```

To disable the automatic export of files to a network server, use the **no** form of the command.

Reloading the Guard

You can reload the Guard configuration without rebooting the machine by using the **reload** command.

For the following changes to take effect, you must reload the Guard:

- Synchronizing the Guard with an NTP server
- Deactivating or activating a physical interface using the **shutdown** command

- Enabling the giga0 interface using the **no shutdown** command
- Burning a new flash

Rebooting the Guard and Inactivating Zones

You can reboot the Guard by using the following command in global mode:

```
reboot
```

By default, the Guard loads all zones in an inactive operation state. The Guard does not enable zone protection or the learning process after reboot, regardless of the zone operation state prior to the reboot.

To allow the Guard to automatically activate zones that were active prior to the reboot process, enter the following command in configuration mode:

```
boot reactivate-zones
```



Caution

The zone learning phase is restarted after reboot.

Shutting Down the Guard

A clean shutdown enables the Guard to save vital information.

To shut down the Guard, perform the following steps:

-
- Step 1** Enter the following command:
- ```
poweroff
```
- Step 2** Type **yes** at the command prompt to verify the process.
- Step 3** Push the Guard power control button to turn the power off. The green power LED turns off.



**Caution**

---

Pushing the power control button without entering the **poweroff** command may result in critical data loss.

---

## Upgrading the Guard Software Version

To upgrade the Guard software version, perform the following steps:

- 
- Step 1** Back up the Guard configuration before initiating the upgrade process by using the **copy running-config** command. Backing up enables you to save your existing configuration so that you can quickly restore the configuration to the current state if needed. See the [“Exporting the Configuration” section on page 13-2](#) for more information.

- Step 2** Export files that you want to save. You can export the following files:
- Export attack reports that you want to save by using the **copy reports** command or the **copy zone zone-name reports** command. See the “Exporting Attack Reports of All Zones” section on page 11-12 and the “Exporting Zone Reports” section on page 11-13 for more information.
  - Export logs that you want to save by using the **copy log** command. See the “Exporting the Log File” section on page 12-8 for more information.
  - Export the packet-dump capture files that you want to save by using the **copy zone zone-name packet-dump captures** command. See the “Exporting Packet-Dump Capture Files Manually” section on page 12-15 for more information.
- Step 3** Upgrade to the latest software release by locating the software image on [www.cisco.com](http://www.cisco.com) and copy the software image to a remote server that is accessible to FTP, SFTP, or SCP.
- Step 4** Copy the software image from the remote server to the Guard software from the network server by entering one of the following commands in global mode:
- **copy ftp new-version server full-file-name [login [password]]**
  - **copy {scp | sftp} new-version server full-file-name login**

Table 13-5 provides arguments for the **copy new-version** command.

**Table 13-5 Arguments for the copy new-version Command**

| Parameter             | Description                                                                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ftp</b>            | Specifies FTP.                                                                                                                                                                                                |
| <b>sftp</b>           | Specifies SFTP.                                                                                                                                                                                               |
| <b>scp</b>            | Specifies SCP.                                                                                                                                                                                                |
| <i>server</i>         | IP address of the server.                                                                                                                                                                                     |
| <i>full-file-name</i> | Complete name of the file. If you do not specify a path, the server copies the file from your home directory.                                                                                                 |
| <i>login</i>          | Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password. |
| <i>password</i>       | (Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.                                                                                               |



**Note**

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-25 for more information.

- Step 5** Install the downloaded version by entering the following command:
- ```
install new-version
```

When you enter the **install new-version** command, the learning and the protection processes are deactivated.

**Caution**

During the upgrade process, you must be sure that there is a stable power supply to the Guard and avoid performing any Guard operations until the Guard displays the following message: “Press Enter to close this CLI session.” If you fail to adhere to these restrictions, the upgrade may fail and cause the Guard to become inaccessible.

Step 6

Establish a new session with the Guard and check the software version by entering the **show version** command.

The following example shows how to copy a new software version file to the Guard and then to upgrade the software version:

```
user@GUARD# copy ftp new-version 10.0.0.191 /home/Versions/R3.i386.rpm user <password>
FTP in progress...
user@GUARD# install new-version
```

.
.
.

Press Enter to close this CLI session.

**Note**

When you upgrade the software version, the Guard updates the self-protection configuration. We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current version.

Burning a New Flash Version to Upgrade the Common Firmware Environment

You can burn a new flash version only when there is a mismatch between the current Common Firmware Environment (CFE) and the software release. A mismatch condition can occur when you update the Guard software.

When a CFE mismatch is detected, the Guard displays the following message when you enter the **install new-version** command (X denotes the old flash version and Y denotes the new flash version): “Bad CFE version (X). This version requires version Y.”

**Caution**

You must be sure that there is a stable power supply to the Guard and avoid performing any Guard operations while you burn a new flash version. If you fail to adhere to these restrictions, the upgrade may fail and cause the Guard to become inaccessible.

To burn a new flash version, perform the following steps:

Step 1

Enter the following command in configuration mode:

```
flash-burn
```

If you try to burn a new flash version when the CFE and the Guard software versions match, the operation fails.

Step 2 Reload the Guard by entering the following command:

```
reload
```

You must enter the **reload** command after burning a new flash version. The Guard is not fully functional until you enter the **reload** command.

The following example shows how to burn a new flash version:

```
user@GUARD-conf# flash-burn
Please note: DON'T PRESS ANY KEY WHILE IN THE PROCESS!
. . .
Burned firmware successfully
SYSTEM IS NOT FULLY OPERATIONAL. Type 'reload' to restart the system
```

Resetting the Linux root or Guard admin User Account Password

You can reset the password associated with the Guard default admin user account using the Linux root user account. This may be necessary if you forget the password for the admin user account and another user with administrative privileges is not available. If another user with administrative privileges is available, see the [“Changing the Passwords of Other Users”](#) section on page 3-8.

To log in as the Linux root user, you must know the password associated with this account, which is encrypted and can only be replaced by a new password. This section shows how to reset the Linux root user password (if needed) to allow you to log in as the root user and reset the Guard default admin user password.

This section contains the following topics:

- [“Resetting the Linux root User Account Password”](#)
- [“Resetting the Guard Default admin User Account Password”](#)

Resetting the Linux root User Account Password

To reset the Linux root user account password, perform the following steps:

-
- Step 1** Attach a keyboard and a monitor to the Guard.
- Step 2** Log in as a Guard user with administrative or configuration privileges and enter the **reboot** command. If you have forgotten all passwords associated with user accounts having administrative or configuration privileges, press CTRL-ALT-DEL to reboot the Guard.
- Step 3** Press down and hold the **Shift** key while the Guard is powering up.
- The Guard displays the following prompt:
- ```
Lilo:
```
- Step 4** Enter the following command to load a single user image:
- ```
Cisco 1
```



Note If you are running a version previous to 3.0.8, enter **Riverhead 1**. If you do not know which version you are running, press the **Tab** key to see the list of images.

- Step 5** Press **Enter** at the password prompt to enter a null password.
The Guard enters the root prompt.
- Step 6** Use the **passwd** command to change the root user account password. Enter a new password at the New password prompt. Reenter the new password at the “Retype new password” prompt to verify your choice.
The following example shows how to change the root password:
- ```
[root@GUARD root]# passwd
Changing password for user root.
New password: <new password typed in here>
Retype new password: <new password typed in here>
passwd: all authentication tokens updated successfully.
```
- Step 7** Restart the Guard in normal operational mode by using the **reboot** command.

If you also need to reset the Guard default admin user account password, see the [“Resetting the Guard Default admin User Account Password”](#) section.

## Resetting the Guard Default admin User Account Password

To reset the Guard default admin user account password, perform the following steps:

- Step 1** Log in to the Guard as the Linux root user. If you have forgotten the password associated with the root user account, see the [“Resetting the Linux root User Account Password”](#) section.
- Step 2** Switch to the admin username by using the **su - admin** command.
- **username admin admin password**—The *password* argument consists of 6 to 24 characters.
  - **password admin**—The CLI prompts you to enter a password and reenter it for verification as shown in the following example:
- ```
@PGuardR3#password admin
New Password:
Retype New Password:
finished successfully
Password was changed successfully
```
- The password consists of 6 to 24 characters.
- Step 3** Switch back to the root prompt by using the **exit** command.
- Step 4** Log out of root using the **exit** command.
- Step 5** Log in to the Guard using the **admin** username and the new password.
- Step 6** (Optional) Configure the other Guard user account names and passwords if required (see the [“Adding a User”](#) section on page 3-6).

Resetting the Guard Configuration to Factory Defaults

You can reset the Guard to the factory-default settings and configure it as a new Guard by using the following command in configuration mode:

```
clear config all
```

Resetting the configuration to factory defaults is useful when you want to remove an undesirable configuration in the Guard, if the configuration has become complex, or if you want to move the Guard from one network to another network.



Caution

Resetting the Guard configuration deletes all configured user account information, including all usernames and associated passwords. After you reset the Guard configuration, the default user accounts (root, admin, and riverhead) are the only user accounts that remain, requiring you to log on using the procedure in the [“Accessing the Guard for the First Time”](#) section on page 2-6.

We recommend that you back up the Guard configuration before you reset it to the factory-default settings by using the **copy running-config** command. See the [“Exporting the Configuration”](#) section on page 13-2.

The out-of-band interface configurations for eth0 and eth1 are available until you reboot the Guard.

To reset the Guard to the factory-default configuration, perform the following steps:

-
- Step 1** Enter the **clear config all** command from the configuration mode. The CLI displays a verification prompt that asks you to verify that you want to clear all of the configuration information.
 - Step 2** Enter **yes**. The CLI displays a prompt stating that a reboot is required and to press the Enter key.



Caution

You must reboot the Guard at this time (using the current session) or the Guard will not operate correctly.

- Step 3** Press the **Enter** key. The Guard reboots to the factory-default settings.
 - Step 4** Access the Guard by following the procedure in the [“Accessing the Guard for the First Time”](#) section on page 2-6.
 - Step 5** (Optional) Configure the other Guard user account names and passwords (see the [“Adding a User”](#) section on page 3-6).
-

The following example shows how to reset the Guard to the factory-default settings:

```
user@GUARD-conf# clear config all
Are you sure you want to clear ALL configuration and logging information?
Type 'yes' to clear config, or any other key to cancel
yes
```

```
Reboot is required after clear config. Please press Enter to continue
```