



CHAPTER 12

Performing Maintenance Tasks

This chapter describes how to perform tasks used for general care and maintenance of the Cisco Traffic Anomaly Detector (Detector).

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector can also synchronize zone configurations with the Guard. For more information about the Guard, see the *Cisco Anomaly Guard Module Configuration Guide* or the *Cisco Guard Configuration Guide*.

This chapter contains the following sections:

- [Configuring File Servers](#)
- [Exporting the Configuration](#)
- [Importing and Updating the Configuration](#)
- [Exporting Files Automatically](#)
- [Reloading the Detector](#)
- [Rebooting the Detector and Inactivating Zones](#)
- [Shutting Down the Detector](#)
- [Upgrading the Detector Software Version](#)
- [Resetting the Linux root or Detector admin User Account Password](#)
- [Resetting the Detector Configuration to Factory Defaults](#)

Configuring File Servers

You can define a network server on the Detector for importing and exporting files between the Detector and the server. The Detector 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** command to configure the Detector 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 12-1 provides the arguments and keywords for the **file-server** command.

Table 12-1 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 string length is 80 alphanumeric 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 Detector authenticates network servers that use SFTP and SCP using a public key.



Note

Because SFTP and Secure Copy Protocol SCP rely on Secure Shell (SSH) for secure communication, you must configure the SSH key that the Detector uses for SFTP and SCP communication. See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-27 for more information.

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

```
user@DETECTOR-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 Detector configuration file or a zone configuration file (running-config) to a network server. By exporting the Detector or zone configuration file to a remote server, you can do the following:

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

To export the Detector 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**

To export the portion of the zone configuration that is required to configure the zone on a Guard, use the **copy guard-running-config** command. See the “Exporting a Zone Configuration Manually to a Network Server” section on page 4-16 for more information.

Table 12-2 provides the arguments and keywords for the **copy running-config ftp** command.

Table 12-2 Arguments and Keywords for the copy running-config ftp Command

Parameter	Description
zone zone-name	(Optional) Specifies the zone name. If you specify the zone name, the Detector exports the zone configuration file. The default is to export the Detector configuration file.
running-config	Exports the complete Detector configuration or the configuration of the specified zone.
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 saves 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 Detector prompts you for one.
<i>file-server-name</i>	Name of a network server to which to export the configuration file. You must configure the network server using the file-server command (see the “Configuring File Servers” section on page 12-1).
<i>dest-file-name</i>	Name of the configuration file on the remote server. The Detector 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 file-server command.



Note

If you configured the network server using SFTP or SCP, you must configure the SSH key that the Detector uses for SFTP and SCP communication. If you do not configure the key that the Detector uses before you enter the **copy** command with the **sftp** or **scp** option, the Detector prompts you for the password. See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-27 for more information.

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

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

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

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

Importing and Updating the Configuration

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

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

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



Note

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

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

To import a Detector 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 12-3 provides the arguments for the **copy ftp running-config** command.

Table 12-3 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 Detector prompts you for one.

Table 12-3 Arguments for the copy ftp running-config Command (continued)

Parameter	Description
<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 12-1).
<i>source-file-name</i>	Name of the file to import. The Detector 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 Detector uses for SFTP and SCP communication. If you do not configure the key that the Detector uses before you enter the **copy** command with the **sftp** or **scp** option, the Detector prompts you for the password. See the “[Configuring the Keys for SFTP and SCP Connections](#)” section on page 3-27 for more information.

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

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

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

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

Exporting Files Automatically

You can configure the Detector to export the following files automatically to a network server:

- Packet-dump capture files—The Detector 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 11-14 for more information.
- Attack reports—The Detector 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 10-6 for more information.
- Zone configuration—The Detector exports the zone configuration file each time that the results of the threshold-tuning phase of the learning process are accepted. See the “[Exporting a Zone Configuration Automatically to a Network Server](#)” section on page 4-15 for more information.

The Detector 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 12-1 for more information.
- Step 2** Configure the Detector to export files automatically by entering the following command:

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

Table 12-4 provides the arguments and keywords for the **export** command.

Table 12-4 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 Detector 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 11-9 for more information about packet-dump capture files.
reports	Exports attack reports in XML format at the end of an attack. The Detector 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 10-6 for more information.
sync-config	Exports the zone configuration each time that the results of the threshold-tuning phase of the learning process are accepted. You can then import the configuration to a Guard and activate it to protect the zone. To enable the Detector to export the zone configuration to a network server automatically, you must configure the server in either the Detector default remote server list or the zone remote server list. See the “ Exporting a Zone Configuration Automatically to a Network Server ” section on page 4-15 for more information.
file-server-name	Name of the network server on which you can save files. Configure the network server using the file-server command (see the “ Configuring File Servers ” section on page 12-1).

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

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

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

To display the default list of network servers to which the Detector exports zone configuration, use the **show sync-config file-servers** command in configuration mode.

To display the zone remote server list, use the **show sync-config file-servers** command in zone configuration mode.

Reloading the Detector

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

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

- Synchronizing the Detector 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 Detector and Inactivating Zones

To reboot the Detector, enter the following command in global mode:

```
reboot
```

By default, the Detector reactivates zones that were active before the reboot process.

To change the default behavior so that the Detector loads all zones in an inactive operation state, enter the following command in configuration mode:

```
no boot reactivate-zones
```



Caution

The zone learning phase is restarted after reboot.

Shutting Down the Detector

A clean shutdown enables the Detector to save vital information.

To shut down the Detector, 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 Detector 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 Detector Software Version

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

- 
- Step 1** Back up the Detector 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 12-2 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 10-7 and the “Exporting Zone Reports” section on page 10-8 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 11-8 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 11-15 for more information.

**Step 3** Upgrade to the latest software release by locating the software image on [www.cisco.com](http://www.cisco.com).

Copy the software image to a directory that is accessible to FTP, SFTP, or SCP.

**Step 4** Copy the software version to the Detector 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 {sftp | scp} new-version server full-file-name login**

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Detector uses before you enter the **copy** command with the **sftp** or **scp** option, the Detector prompts you for the password. See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-27 for more information about how to configure the key that the Detector uses for secure communication.

Table 12-5 provides the arguments and keywords for the **copy new-version** command.

**Table 12-5 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>          | (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 Detector prompts you for one.                                                                                                       |

**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 detection processes are deactivated.

**Caution**

You must be sure that there is a stable power supply to the Detector, and avoid performing any Detector operations while you upgrade the version. After the upgrade process finishes, the Detector 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 Detector to become inaccessible.

**Step 6**

Establish a new session with the Detector 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 Detector and then upgrade the software version:

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

Press Enter to close this CLI session.

## Burning a New Flash Version

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 Detector software.

**Note**

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

When a CFE mismatch is detected, the Detector 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 Detector and avoid performing any Detector operations while you burn a new flash version. If you fail to adhere to these restrictions, the upgrade may fail and cause the Detector to become inaccessible.

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

**Step 1**

Enter the following command in configuration mode:

```
flash-burn
```

**Step 2** Reload the Detector by entering the following command:

```
reload
```

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

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

```
user@DETECTOR-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 Detector admin User Account Password

You can reset the password associated with the Detector 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 Detector default admin user password.

This section contains the following topics:

- [“Resetting the Linux root User Account Password”](#)
- [“Resetting the Detector 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 Detector.

**Step 2** Log in as a Detector 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 Detector.

**Step 3** Press down and hold the **Shift** key while the Detector is powering up.

The Detector 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 Detector 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@DETECTOR 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 Detector in normal operational mode by using the **reboot** command.

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

## Resetting the Detector Default admin User Account Password

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

- Step 1** Log in to the Detector 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.
- Step 3** Configure the password for the Detector default admin user account by using one of the following commands:
- **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 4** Switch back to the root prompt by using the **exit** command.
- Step 5** Log out of root using the **exit** command.
- Step 6** Log in to the Detector using the **admin** username and the new password.
- Step 7** (Optional) Configure the other Detector user account names and passwords if required (see the [“Adding a User”](#) section on page 3-7).

Resetting the Detector Configuration to Factory Defaults

You can reset the Detector to the factory-default settings and configure it as a new Detector 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 Detector, if the configuration has become complex, or if you want to move the Detector from one network to another network.

**Caution**

Resetting the Detector configuration deletes all configured user account information, including all usernames and associated passwords. After you reset the Detector 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 Detector for the First Time”](#) section on page 2-7.

We recommend that you back up the Detector 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 12-2.

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

To reset the Detector 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 Detector at this time (using the current session) or the Detector will not operate correctly.

Step 3 Press the **Enter** key. The Detector reboots to the factory-default settings.

Step 4 Access the Detector by following the procedure in the [“Accessing the Detector for the First Time”](#) section on page 2-7.

Step 5 (Optional) Configure the other Detector user account names and passwords (see the [“Adding a User”](#) section on page 3-7).

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

```
user@DETECTOR-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
```

