



CHAPTER 2

Initializing the Detector

This chapter describes the basic tasks required to initialize the Cisco Traffic Anomaly Detector (Detector) in a network and how to manage it.

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:

- [Using the Command-Line Interface](#)
- [Accessing the Detector for the First Time](#)
- [Configuring the Detector Interfaces](#)
- [Configuring the Default Gateway](#)
- [Adding a Static Route to the Routing Table](#)
- [Managing the Detector](#)

Using the Command-Line Interface

You can control the Detector functions by using the command-line interface (CLI). The Detector user interface is divided into many different command modes and the access to the CLI is mapped according to user privilege levels. The commands that are available to you depend on which mode you are currently in.

This section contains the following topics:

- [Understanding User Privilege Levels](#)
- [Understanding Command Modes](#)
- [Entering CLI Commands](#)
- [Tips for Using the CLI](#)

Understanding User Privilege Levels

The access to the CLI is mapped according to user privilege levels. Each privilege level has its own group of commands.

Table 2-1 describes the user privilege levels.

Table 2-1 User Privilege Levels

User Privilege Level	Description
Administration (admin)	Provides access to all operations.
Configuration (config)	Provides access to all operations except for operations relating to user definition, deletion, and modification.
Dynamic (dynamic)	Provides access to monitoring and diagnostic operations, detection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters.
Show (show)	Provides access to monitoring and diagnostic operations.



Note

We recommend that users with Administration and Configuration privilege levels configure all filters. Users with lower privilege levels can add and remove dynamic filters.

Understanding Command Modes

This section contains summaries of the command and configuration modes used in the Detector CLI. To obtain a list of commands available for each command mode, enter ? at the system prompt.

Table 2-2 lists and describes the Detector command modes.

Table 2-2 Detector Command Configuration Modes

Mode	Description
Global	Allows you to connect to remote devices and list system information. The Global prompt is the default prompt when you log into the Detector. The command prompt is as follows: user@DETECTOR#
Configuration	Allows you to configure features that affect the Detector operations and have restricted user access. To enter configuration mode, use the configure command in global mode. The command prompt is as follows: user@DETECTOR-conf#
Interface configuration	Allows you to configure the Detector networking interfaces. To enter interface configuration mode, use the interface command in configuration mode. The command prompt is as follows: user@DETECTOR-conf-if-<interface-name>#

Table 2-2 *Detector Command Configuration Modes (continued)*

Mode	Description
Router configuration	<p>Allows you to configure the Detector routing configuration.</p> <p>To enter router configuration mode, use the router command in configuration mode. The command prompt is as follows:</p> <pre>router></pre>
Zone configuration	<p>Allows you to configure the zone attributes.</p> <p>To enter zone configuration mode, use the zone command in configuration mode or use the configure command in global mode. The command prompt is as follows:</p> <pre>user@DETECTOR-conf-zone-<zone-name>#</pre>
Policy template configuration	<p>Allows you to configure the zone policy templates.</p> <p>To enter policy template configuration mode, use the policy-template command in zone configuration mode. The command prompt is as follows:</p> <pre>user@DETECTOR-conf-zone-<zone-name>-policy_template-<policy-template-name>#</pre>
Policy configuration	<p>Allows you to configure the zone policies.</p> <p>To enter policy configuration mode, use the policy command in zone configuration mode. The command prompt is as follows:</p> <pre>user@DETECTOR-conf-zone-<zone-name>-policy-<policy-path>#</pre>
Guard configuration	<p>Allows you to configure the zone definitions that are unique to the Guard, such as user filters.</p> <p>To enter guard configuration mode, use the guard-conf command in zone configuration mode. The command prompt is as follows:</p> <pre>user@DETECTOR-conf-zone-<zone-name> (guard) #</pre>

Entering CLI Commands

This section contains the following topics:

- [Using the no Form of a Command](#)
- [show Command Syntax](#)
- [CLI Error Messages](#)

Table 2-3 describes the rules for entering CLI commands.

Table 2-3 *CLI Rules*

Action	Keyboard Sequence
Scroll through and modify the command history	Use the arrow keys.
Display commands available in a specific command mode	Press Shift and enter the ? (question mark) key

Table 2-3 CLI Rules (continued)

Action	Keyboard Sequence
Display a command completion	Type the beginning of the command and press Tab .
Display a command syntax completion(s)	Enter the command and press Tab twice.
Scroll using the more command	Enter the more number-of-lines command. The more command configures the number of additional lines displayed in the window once you press the Spacebar. The default is two lines less than the capability of the terminal. The <i>number-of-lines</i> argument configures the number of additional lines to be displayed once you press the Spacebar.
Scroll on a single screen (within a command output)	Press the Spacebar .
Scroll back a single screen (within a command output)	Press the b key.
Stop scroll movement	Press the q key.
Search forward for a string	Press the / (slash mark) key and enter the <i>string</i> .
Search backward for a string	Press the ? (question mark) key and enter the <i>string</i> .
Cancel the action or delete a parameter	Use the no form of a specific command.
Display information relating to a current operation	Enter the show command.
Exit from a current command group level to a higher group level	Enter the exit command.
Exit all command group levels and return to the root level	Enter the end command.
Display command output from and including the first line that contains a <i>string</i>	Enter the (vertical bar) and then enter the begin string command.
Display command output lines that include a <i>string</i>	Enter the (vertical bar) and then enter the include string command.
Display command output lines that do not include a <i>string</i>	Enter the (vertical bar) and then enter the exclude string command.

**Note**

If you enter the **exit** command at the root level, you exit the CLI environment to the operating system login screen.

Using the no Form of a Command

Almost every configuration command also has a **no** form. In general, use the **no** form of a command to disable a feature or function. Use the command without the keyword **no** to enable a disabled feature or function. For example, the **event monitor** command turns on the event monitor, and the **no event monitor** command turns it off.

show Command Syntax

You can execute zone-related **show** commands from the zone configuration mode. Alternatively, you can execute these commands from the global or configuration modes.

The following is the syntax for the **show** command in global or configuration modes:

```
show zone zone-name parameters
```

The following is the syntax for the **show** command in zone configuration mode:

```
show parameters
```

**Note**

This publication uses the **show** command syntax from the zone configuration mode unless explicitly specified.

CLI Error Messages

The Detector CLI displays error messages in the following situations:

- The syntax of the command is incomplete or incorrect.
- The command does not match the system configuration.
- The operation could not be performed due to a system failure. In this situation, an entry is created in the system log.

Tips for Using the CLI

This section provides tips for using the CLI and contains the following topics:

- [Using Help](#)
- [Using Tab Completion](#)
- [Understanding Conventions of Operation Direction](#)
- [Abbreviating a Command](#)
- [Using Wildcard Characters](#)

Using Help

The CLI provides context-sensitive help at every mode of the command hierarchy. The help information tells you which commands are available at the current command mode and provides a brief description of each command.

To get help, type `?`.

To display help for a command, type `? after the command.`

To display all commands available in a mode along with a short description, enter `? at the command prompt.`

The help displays commands available in the current mode only.

Using Tab Completion

You can use tab completion to reduce the number of characters that you need to type for a command. Type the first few characters of a command and press **Tab** to complete the command.

After entering a command that has a value with multiple options, press **Tab** twice to display a list of possible input parameters, including system-defined parameters and user-defined parameters. For example, if you press **Tab** twice after entering the **policy-template** command in zone configuration mode, the list of policy template names is displayed. If you press **Tab** twice after entering the **zone** command in configuration mode, zones that are already defined are displayed.

If multiple commands match for a Tab completion action, nothing is displayed; the system repeats the current line that you entered.

The tab completion feature displays only commands available for the current mode.

You can disable tab completion for zone names in all commands in global and configuration modes such as the **zone** command and the **show zone** commands by using the **aaa authorization commands zone-completion tacacs+** command. See the [“Disabling Tab Completion of Zone Names” section on page 3-13](#) for more information.

Understanding Conventions of Operation Direction

The order of keywords in the command syntax defines the direction of the operation. When you enter the keyword before you enter the command, the Detector copies the data from the Detector to the server. When you enter the command before you enter the keyword, the Detector copies the data from the server to the Detector. For example, the **copy log ftp** command copies the log file from the Detector to the FTP server. The **copy ftp new-version** command copies the new software version file from the FTP server to the Detector.

Abbreviating a Command

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation.

For example, you can abbreviate the **show** command to **sh**.

Using Wildcard Characters

You can use an asterisk (*) as a wildcard.

For example, if you enter the **permit wbm *** command, you allow all remote manager IP addresses to access the Detector using the Web-Based Manager (WBM).

If you enter the **learning policy-construction scan*** command, the policy construction phase is activated for all the zones that are configured on the Detector with names that begin with scan (such as scannet, scanserver, and so on).

If you enter the **no zone *** command, **all zones are removed**.

Accessing the Detector for the First Time

This section shows how to establish the initial session with the Detector by using the preconfigured username that has an administration user privilege level. During this process, the CLI prompts you to assign passwords to the following default user accounts:

- **admin**—Provides access to all administrative and configuration operations.
- **riverhead**—Provides access to monitoring and diagnostic operations, zone protection, and learning-related operations. This user can also configure flex-content filters and dynamic filters.
- **root**—Provides access to the Linux shell for certain administrative operations.

To access the Detector for the first time, perform the following steps:

-
- Step 1** Press the power control button on the front of the Detector. During power-up, the green power LED on the front of the Detector is on.
- After the Detector boot process finishes, the software prompts you to enter a username.
- Step 2** Enter **admin** for the username and **rhadmin** for the password.
- Step 3** Enter a password for the root user account that consists of 6 to 24 characters.
Retype the new password to verify it.
- Step 4** Choose a password for the admin user account that consists of 6 to 24 characters.
Retype the new password to verify it.
- Step 5** Enter a password for the riverhead user account that consists of 6 to 24 characters.
Retype the new password to verify it.



Note You can change the passwords for the admin and riverhead user accounts at any time. See the [“Changing Your Password” section on page 3-7](#) for more information.

- Step 6** Enter configuration mode to configure the Detector by entering the following command:

```
configure [terminal]
```

The following example shows how to enter configuration mode:

```
user@DETECTOR# configure  
user@DETECTOR-conf#
```

Configuring the Detector Interfaces

The Detector has several Network Interface Cards (NICs). The eth0 and the eth1 10/100/1000 Ethernet interfaces comprise the out-of-band NICs used for management purposes.

The giga0 and the giga1 Gigabit Ethernet interfaces comprise the in-band NICs that the Detector uses for zone traffic reception.



Caution

You must activate the Detector in-band interfaces even though you cannot assign an IP address to them because they are connected to the network in promiscuous mode. See the “[Configuring a Physical Interface](#)” section on page 2-8 for more information.

You must configure the Detector interfaces so that the Detector can operate correctly. Many features are enabled on a per-interface basis. When you enter the **interface** command, you must specify the interface type and number.

Follow these guidelines for all physical and virtual interface configuration processes:

- The eth0 or eth1 out-of-band interface must be configured with an IP address and subnet mask. If required, you can configure both eth0 and eth1 interfaces.
- You must activate each interface using the **no shutdown** command.

To display the status or configuration of an interface, enter the **show** or **show running-config** commands in the interface configuration mode.

This section contains the following topics:

- [Configuring a Physical Interface](#)
- [Clearing the Counters of a Physical Interface](#)

Configuring a Physical Interface

To connect the Detector to a network, configure a physical interface.

The Detector has four physical interfaces: eth0, eth1, giga0, and giga1. The out-of-band interfaces are eth0 and eth1 (10/100/1000 Ethernet sockets for out-of-band management). The in-band interfaces (copper or fiber socket) are giga0 and giga1.



Caution

Do not configure two interfaces on the same subnet or the Detector routing may not work properly.

To configure a physical interface, perform the following steps:

Step 1 Enter interface configuration mode by entering the following command in configuration mode:

```
interface if-name
```

The *if-name* argument specifies the interface name. The Detector supports the following interfaces:

- eth0 or eth1—Out-of-band interfaces
- giga0 or giga1—In-band interfaces

- Step 2** On the eth0 or eth1 out-of-band interface only, set the interface IP address by entering the following command:
- ```
ip address ip-addr ip-mask
```
- The *ip-addr* and *ip-mask* arguments define the interface IP address. Enter the IP address and subnet mask in dotted-decimal notation (for example, an IP address of 192.168.100.1 and a subnet mask of 255.255.255.0).
- Step 3** (Optional) Define the interface maximum transmission unit (MTU) by entering the following command:
- ```
mtu integer
```
- The *integer* argument is an integer between 576 and 1800 for all interfaces. The default MTU value is 1500 bytes.
- Step 4** (Optional) On the giga0 or giga1 in-band interface only, configure the interface speed and duplex mode by entering the following command:
- ```
speed {auto | half speed | full speed}
```

Table 2-4 provides the arguments and keywords for the **speed** command.

**Table 2-4 Arguments and Keywords for the speed Command**

| Parameter    | Description                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto</b>  | Turns on the interface autonegotiation capability. The interface automatically operates at 10/100/1000 Mbps and at half or full duplex, depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration. This mode is the default. |
| <b>half</b>  | Specifies half-duplex operation.                                                                                                                                                                                                                                                                                                    |
| <b>full</b>  | Specifies full-duplex operation.                                                                                                                                                                                                                                                                                                    |
| <i>speed</i> | Interface speed. Enter <b>10</b> , <b>100</b> , or <b>1000</b> for 10 Mbps, 100 Mbps, and 1000 Mbps.                                                                                                                                                                                                                                |

- Step 5** Activate the interface by entering the following command:
- ```
no shutdown
```

After activating or deactivating a giga0 or giga1 in-band interface, you must reload the Detector for the configuration change to take effect.

The following example shows how to configure and activate interface eth1:

```
user@DETECTOR-conf# interface eth1
user@DETECTOR-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
user@DETECTOR-conf-if-eth1# no shutdown
```

To deactivate a physical interface, use the **shutdown** command.

Clearing the Counters of a Physical Interface

You can clear the counters of physical interfaces that are used for data traffic (that is, the Gigabit Ethernet interfaces) if you are going to perform testing and want to be sure that the counters include information from the testing session only.

To clear the interface counters, use the following command in interface configuration mode:

```
clear counters
```

The following example shows how to clear the counters of the interface giga2:

```
user@DETECTOR-conf-if-giga2# clear counters
```

Configuring the Default Gateway

The default gateway receives and forwards packets that have IP addresses that are unknown to the local network. In most cases, the Detector default gateway IP address is the adjacent router, located between the Detector and the Internet. The default gateway address must be on the same network as one of the IP addresses of the Detector network interfaces.

To assign a default gateway address, use the following command in configuration mode:

```
default-gateway ip-addr
```

The *ip-addr* argument specifies the default gateway IP address. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1).

To modify the default gateway address, reenter the command.

The following example shows how to configure the default gateway:

```
user@DETECTOR-conf# default-gateway 192.168.100.1
```

Adding a Static Route to the Routing Table

You can add a static route to the Detector routing table. Add a static route to specify routes for servers or networks outside the local networks that are associated with the Detector IP interfaces. The static route is added permanently and is not removed after the Detector is rebooted.

To add a static route to the Detector routing table, use the following command in configuration mode:

```
ip route ip-addr ip-mask nexthop-ip [if-name]
```

Table 2-5 provides the arguments for the **ip route** command.

Table 2-5 Arguments for the ip route Command

Parameter	Description
<i>ip-addr</i>	Network destination of the route. The destination can be an IP network address (where the host bits of the network address are set to 0) or an IP address for a host route. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
<i>ip-mask</i>	Subnet mask associated with the network destination. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).

Table 2-5 Arguments for the ip route Command (continued)

Parameter	Description
<i>nexthop-ip</i>	Forwarding or next-hop IP address over which the set of addresses that are defined by the network destination and subnet mask are reachable. The next-hop IP address should be within the interface subnet. For local subnet routes, the next-hop IP address is the IP address that is assigned to the interface that is attached to the subnet. For remote routes, available across one or more routers, the next-hop IP address is a directly reachable IP address that is assigned to a neighboring router.
<i>if-name</i>	(Optional) Interface on the Detector over which the destination is reachable. If you do not specify an interface, the next-hop IP address in the Detector routing table determines the interface used.

The following example shows how to configure a static route:

```
user@DETECTOR-conf# ip route 172.16.31.5 255.255.255.255 192.168.100.34
```

To display the routing table, enter the **show ip route** command.

Managing the Detector

Initially you can manage the Detector locally from a console. The console connection provides access to the CLI and allows you to run the initial setup procedures when you first turn on the Detector. See the [“Assigning Privilege Levels with Passwords” section on page 3-10](#) for more information.

After you configure the Detector networking (see the [“Configuring the Detector Interfaces” section on page 2-8](#)), you can access and manage the Detector using one of the following methods:

- Access using a Secure Shell (SSH) session.
- Access the Detector using a Web-Based Manager (WBM).
- Access the Detector using the Cisco DDoS MultiDevice Manager (MDM).
- Access from a DDoS-sensing network element. Refer to the appropriate documentation for more information.

This section contains the following topics:

- [Managing the Detector with the Web-Based Manager](#)
- [Managing the Detector with the Cisco DDoS MultiDevice Manager](#)
- [Accessing the Detector with SSH](#)

Managing the Detector with the Web-Based Manager

You can manage the Detector using the WBM and a web browser.

To enable the WBM and manage the Detector, perform the following steps:

Step 1 Enable the WBM service by entering the following command in configuration mode:


```
service wbm
```

- Step 2** Permit access to the Detector from the remote manager IP address by entering the following command in configuration mode:

```
permit wbm {* | ip-addr [ip-mask]}
```

Table 2-6 provides the arguments for the **permit wbm** command.

Table 2-6 Arguments for the permit wbm Command

Parameter	Description
*	Asterisk wildcard character that allows access by all remote manager IP addresses.
	 <p>Caution For security reasons, we recommend that you not permit access to a service from all IP addresses.</p>
<i>ip-addr</i>	IP address of the remote manager. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
<i>ip-mask</i>	(Optional) Subnet mask. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).

- Step 3** Open the browser and enter the following address:

```
https://Detector-ip-address/
```

The *Detector-ip-address* argument is the IP address of the Detector.

The Detector WBM window appears.



Note HTTPS, not HTTP, is used to enable web-based management control.

- Step 4** Enter your username and password and click **OK**. After you enter the username and password, the Detector home page displays.

If you have the Detector configured to use Terminal Access Controller Access-Control System Plus (TACACS+) authentication, the Detector uses the TACACS+ user database for user authentication instead of its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Detector may prompt you for a new password based on the configuration of the user on the TACACS+ server or notify you when the password is about to expire.

The following example shows how to enable the Detector WBM:

```
user@DETECTOR-conf# service wbm
user@DETECTOR-conf# permit wbm 192.168.30.32
```

Managing the Detector with the Cisco DDoS MultiDevice Manager

The Cisco DDoS MultiDevice Manager (MDM) is a server-based application that allows you to manage one or more Detectors using a web browser. To use the MDM to manage your network of Detectors, perform the following actions:

- Install and configure the MDM software on a network server (see the *Cisco DDoS MultiDevice Manager Configuration Guide*).

- Enable the MDM service on your Detector and permit access by the MDM as described in the following procedure.

To enable the MDM service on the Detector, perform the following steps:

Step 1 Enable the MDM service by entering the following command in configuration mode:

```
service mdm
```

Step 2 Permit access to the Detector from the MDM by entering the following command in configuration mode:

```
mdm server ip-addr
```

The *ip-addr* argument defines the IP address of your MDM server. Enter the IP address in dotted-decimal notation.

The following example shows how to enable the MDM service and permit access by the MDM:

```
user@DETECTOR-conf# service mdm
user@DETECTOR-conf# mdm server 192.168.30.32
```

For information about using the MDM to manage your Detectors, see the *Cisco DDoS MultiDevice Manager Configuration Guide*.

Accessing the Detector with SSH

You can access the Detector using an SSH connection. The SSH service is enabled by default.


To access the Detector with SSH, perform the following steps:

Step 1 Permit access to the Detector from the remote network IP address by entering the following command in configuration mode:

```
permit ssh { * | ip-addr [ip-mask] }
```

[Table 2-7](#) provides the arguments for the **permit ssh** command.

Table 2-7 Arguments for the permit ssh Command

Parameter	Description
*	Asterisk wildcard character that allows access by any remote network.
	 Caution For security reasons, we recommend that you not permit access to all remote networks.
<i>ip-addr</i>	IP address of the remote network. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
<i>ip-mask</i>	(Optional) Subnet mask. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).

Step 2 Establish a connection from the remote network address and enter your login username and password.

If you have the Detector configured to use TACACS+ authentication, the Detector uses the TACACS+ user database for user authentication instead of its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Detector may prompt you for a new password based on the configuration of the user on the TACACS+ server or notify you when the password is about to expire.

To enable the SSH connection without entering a login username and password, perform the following:

- Configure the Detector to use a locally configured login and password for authentication. See the [“Configuring Authentication” section on page 3-5](#) for more information.
 - Add the remote connection SSH public key to the Detector SSH key list. See the [“Managing SSH Keys” section on page 3-25](#) for more information.
-

The following example shows how to enable an SSH connection to the Detector:

```
user@DETECTOR-conf# permit ssh 192.168.30.32
```