



Cisco Traffic Anomaly Detector Operation and Diagnostics

This chapter describes how to perform common monitoring and operational tasks on the Cisco Traffic Anomaly Detector using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Detector Summary \(Home\) Screen](#)
- [Detector Diagnostics](#)
- [User Management](#)—Creating users and viewing users list

For information on zone management, creating zones and viewing zones' status, see [Chapter 4, “Zone Creation and Configuration.”](#)



Note

The Detector must get a copy of the traffic either by using the port-mirroring feature (such as SPAN) of a switch, or by using an optical splitter. Detector configuration, remote Guard list configuration and Networking and configuration can only be assumed using the CLI. Refer to the *Cisco Detector User Guide* for further details.

Detector Summary (Home) Screen

The Detector's summary (home) screen (Figure 3-1) provides a summary of the current Detector activity.

To navigate to the Detector's summary (home) screen:

- Select **Detector Summary** from the navigation pane.
- Select **Home** from the upper right side of the header area.
- Select **Home** from the location bar on the zone pages.

Figure 3-1 Detector Summary (Home) Page

Detector Summary



Zones Under Detection

Zone	Activation time	Attack start time	#DF	#PF	Receive rate
scannet	Dec 18, 19:03:10	Dec 18, 20:31:24	0	20	2041748
MailServer	Dec 18, 21:20:59	N/A	0	N/A	N/A

118245

The Detector Summary includes two sections.

- **Detector Summary**—Provides a summary of received traffic rate, displayed in bits per second (bps), handled by the Detector in the past two hours.

Below the graph, the following information is displayed:

Parameter	Description
Min	Indicates the minimum traffic rate in bps measured in the past two hours
Max	Indicates the maximum traffic rate in bps measured in the past two hours
Avg	Indicates the average traffic rate in bps measured in the past two hours
Cur	Indicates the current traffic rate in bps

- **Zones Under Detection**—Provides a list of the current zones under detection and a short summary of the status of each one of them. The zones are displayed according to the attack order. The most recently attacked zone is displayed at the top of the list.

The following information is provided for each zone:

Parameter	Description
Zone	Indicates the zone name. The zone name also provides a link to the zone's "home page."
Activation Time	Indicates the date and time detection for the zone was initiated.
Attack Start Time	Indicates the date and time the most recent attack on the zone was detected.
Receive Rate	Indicates the current rate traffic, destined to the zone, measured in bps.
Thumbnail of the Zone traffic summary	A graph displaying a summary of the traffic destined to the zone in the past half hour. The traffic rate is displayed in bps.

Detector Diagnostics

You may obtain diagnostics information on the Detector for troubleshooting and monitoring purposes.

To view the Detector's diagnostics:

From the Detector's main menu, select **Diagnostics**.

The following diagnostics are available:

- Counters
- Event Log

Counters

The Detector global counters report (Figure 3-2) provides additional information to the Detector summary displayed in the Detector's "home page."

To display the Detector global counters:

From the Detector's main menu, select **Diagnostics > Counters**.

Figure 3-2 Detector Global Counters/Rates



The Received packets counter provides information on the total amount of packets received and analyzed by the Detector.

The following information is provided:

Parameter	Description
Packets	Indicates the total amount of packets since the Detector was reloaded.
Bits	Indicates the total amount of bits since the Detector was reloaded.
pps	Indicates the current traffic rate measured in packets per second.
bps	Indicates the current traffic rate measured in bits per second.

By default the traffic rate is displayed for a period of the past two hours, measured in bps. Choose the period of time to be displayed and the graph units.

To update the graph according to the settings chosen:

Click **Update Graph** (see [Figure 3-2](#)).

Below the graph the minimum, maximum and average rate are displayed for the period of time and rate units chosen.

Event Log

The Event log ([Figure 3-3](#)) displays monitoring and troubleshooting information. Logs are displayed for events that relate to the detected zones and to the Detector operation.

To display the event log:

From the Detector's main menu, select **Diagnostics > Event log**.

Figure 3-3 Event Log

The screenshot shows the 'Event log' page with the following content:

Event log
Home > Events

Show all Events.

Show events with severity level: Emergency Alert Critical Error Warning Notify [Filter events](#)

First events << Previous events Next events >> Latest events

Time	Issued by	Severity	Type	Details
Dec 18 21:20:59	MailServer	Notify	detection-start	Zone activation completed successfully.
Dec 18 20:42:44	MailServer	Notify	zone-added	Added zone MailServer with id 1007.
Dec 18 20:42:25	ssh[27531]	Notify		Accepted password for admin from 10.0.0.192 port 3853 ssh2

You may choose to filter the events according to their severity level.

The event severity levels are:

Event Level	Description
Emergencies	System is unusable
Alerts	Immediate action required
Critical	Critical condition
Errors	Error condition
Warnings	Warning condition
Notifications	Normal but significant condition
Informational	Informational messages
Debugging	Debugging messages

To filter events according to their severity level:

1. Select the check boxes next to the severity levels.
2. Click **Filter Events**.



Note

The event logs display zone related event logs only with a severity level of Emergency, Alert, Critical, Error, Warning and Notification. See [Chapter 8, “Zone Statistics and Diagnostics,”](#) for further details on zone event logs.

User Management

The access to the Detector is mapped according to user privilege levels. Each user privilege level is granted with a corresponding set of command group operations. [Table 3-1](#) displays the Detector user privilege levels and their corresponding command operation groups:

Table 3-1 *User Privilege Levels*

User Group	Command Group
Administrator (Admin)	Full access to all operations.
Configuration (Config.)	Full access to all operations except the operations relating to user definition, deletion, and modification.
Dynamic	The entire monitoring and diagnostics operations group, the detection, and the learning related operations. Dynamic privileged-users may also configure the Flex and Dynamic filters (see the note below).
Show	The entire monitoring and diagnostics operations group.

**Note**

We recommend that Administrator and Configuration privilege level users perform all filter configuration procedures. Lower privileged users can also perform dynamic filter addition and removal.

The Detector enables the Administrator to configure which authentication method the Detector utilizes when a user tries to log into the Detector. The Detector offers the following authentication options:

- Detector local authentication—Local authentication uses locally configured login passwords for authentication. This is the default authentication method.
- TACACS+ authentication—TACACS+ authentication authenticates users through a TACACS+ server or a list of TACACS+ servers.

**Note**

TACACS+ authentication can only be configured from the CLI. Refer to the “TACACS+ and Local Authentication Methods” section in Chapter 2, “Initial Procedures,” in the *Cisco Traffic Anomaly Detector User Guide*.

Assigning Privilege Level Procedure

A preconfigured Administrator's privilege level is provided, enabling you to define the Detector user types. Defining users enables you to divide the Detector user community into privilege levels.

**Note**

The admin user name grants Administrator's privilege level. The riverhead user name grants the Dynamic privilege level.

Creating Users

An administrator-privileged user may configure local users.

**Note**

If TACACS+ authentication is configured, the TACACS+ user database is used for user authentication rather than the local database. Refer to the “TACACS+ and Local Authentication Methods” section in Chapter 2, “Initial Procedures,” in the *Cisco Traffic Anomaly Detector User Guide*.

To create a new user:

From the main menu, select **Users > Create user**.

For each user define the following:

Parameter	Description
User name	The User's user name.
Initial password	6-24 characters long excluding spaces.
Type	The user's privilege level. From the drop-down list choose: admin, config, dynamic or show, as defined above.

Alternatively, to create a new user:

On the Users list screen (see the [“Users List”](#) section), click **Add**.

Users List

You may view the list of users defined on the Detector.

To view the list of users defined on the Detector:

From the main menu, select **Users > Users list**.

The list of users is divided into two categories:

- System users—Users defined by the system. System users cannot be deleted. The system users are admin and riverhead.
- Users—Users defined by the operator.

To remove a user:

1. Select the check box next to the user name.
2. Click **Delete**.

To add a user:

Click **Add**.

The user's privilege level is displayed for each user (see [Table 3-1](#)).

To reconfigure a user:

Click on the user name.

Changing a Password

To change the password:

1. From the Detector's main menu select **Users > Change password**.
The Change Password window appears.
2. Enter the existing password in the **Old Password** box.
3. Enter a new password in the **New Password** box, and re-enter the new password to verify your choice.
4. Click **OK**.
5. If an invalid password is entered or the new password is not verified correctly, an error message is displayed. Click **Go Back** to try again.

Users that have an Administrator privilege level may configure and change the password of all users defined on the Detector.

To reconfigure or change the passwords of users, other than the current one:

1. From the main menu select **Users > Users list**.
2. Click on the required user name.
3. Click **Config**.
4. Enter the new password.
5. Click **OK**.

Changing the Privilege Level

To change the user privilege level:

- Delete the user (see the [“Users List”](#) section).
- Re-create the user (see the [“Creating Users”](#) section).