



WBM Basic Procedures

This chapter provides an overview of the Web-Based Management (WBM) basic procedures.

This chapter includes the following sections:

- [Setting Up the WBM](#)—Provides an explanation on how to enable the WBM in the Detector and how to connect to the Detector's WBM
- [Guard Remote Activation](#)—Provides an explanation on how to configure the Detector to remotely activate the Guard upon traffic anomaly detection

Setting Up the WBM

Before setting up the WBM, some basic configuration of the Detector needs to be performed. The following information at a minimum must be known for the Detector to be managed:

- The IP address of the Detector
- Admin or config privileged user-name and password



Note

Admin and config privileged users can configure WBM access for dynamic and show privilege users.

Enabling WBM on the Detector

For detailed information on the Guard's CLI, refer to the *Cisco Traffic Anomaly Detector User Guide*.

Enable the WBM Service

To enable the Detector WBM service, perform the following from the Detector's command line interface:

1. From the Configuration command group level type the following:

```
service wbm
```

2. Press **ENTER**. The following screen appears:

```
admin@DETECTOR-conf> service wbm  
admin@DETECTOR-conf>
```

To disable the WBM service:

From the Configuration command group level type the following:

```
no service wbm
```

Granting Access Permission to the WBM Service

To Grant permission for an IP address to access the Detector's WBM service perform the following:

1. From the Configuration command group level type the following:

```
permit wbm <ip-addr> [<ip-mask>]
```

Where:

- *<ip-addr>*—Indicates the IP address of the permitted user, that is, the IP address of the manager. Use * to indicate any IP address.
 - *<ip-mask>]*—(Optional) Indicates the IP mask of the permitted user.
2. Press **ENTER**. The following screen appears:

```
admin@DETECTOR-conf> permit wbm 10.0.0.192 255.255.255.240  
admin@DETECTOR-conf>
```

**Note**

We do not recommend permitting WBM access from any IP address after initial configuration due to security considerations.

To deny WBM access from a remote manager:

From the Configuration command group level type the following:

```
no permit wbm <ip-addr> [<ip-mask>]
```

Connecting From the Manager's Station

To connect to the Detector WBM perform the following:

1. In the remote station, open the browser window.
2. Enter the Detector's IP address in the browser's address bar. Connect using **https** as shown below:

```
https://<ip-address>
```

**Note**

https and not http is used.

The following login screen appears:

3. Type your username and password.
4. Click **OK**.

An error message appears if the user name or password entered is incorrect.

After the user name and password are entered correctly, the Detector's main screen is displayed (see [Figure 1-1](#)).



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*.

If you fail to connect to the Detector:

- Make sure the correct user name and password are entered.
- Make sure the correct IP address is entered in the URL field of the browser and that you connected using https.
- Check the network connections of both the remote manager's station and the Detector.

- Try to connect to the Detector using ssh and see if it is indeed reachable.
- Verify that the WBM service is enabled and that access from the remote manager's IP address is permitted.

Guard Remote Activation

When the Detector detects a zone traffic anomaly, it activates a remote Guard or Guards or logs the event (an action known as “notify”). Those Guards initialize protection measures to protect the zone.

**Note**

Remote Guard list configuration can only be assumed using the CLI.

A list of the remote Guards to be activated is defined when configuring the zone (refer to the “Zone Remote Guard List” section in Chapter 4, “Zone Configurations,” in the *Cisco Traffic Anomaly Detector User Guide*) or when configuring the Detector default list. The Detector first turns to the zone-configured remote Guard list and then, if nothing is specified, to the default list.

**Note**

The Guard lists (default and zone specific) may contain one or more Guards.

This section describes the default remote Guard list configuration procedures.

Refer to the refer to the “Zone Remote Guard List” section in Chapter 4, “Zone Configurations,” in the *Cisco Traffic Anomaly Detector User Guide* for further details.

Adding a Guard to the Default Remote List

You may configure one or more Guards to be remotely activated upon traffic anomaly detection.



Note

The list should contain at least one value in case no Guards are defined at zone configuration. When no remote Guards are defined in both lists, the Detector would record the event in its syslog.

To add a Guard to the remote Guard list perform the following:

From the Configuration command group level type the following:

```
admin@DETECTOR-conf> remote-guard <remote-guard-address>
admin@DETECTOR-conf>
```

The command syntax is:

```
remote-guard {<remote-guard-address>|*} <description>
```

Where:

- *<remote-guard-address>*—Indicates the remote Guard IP address. To remove all Guard IP addresses from the list use * with **no**.
- *description*—(Optional) Indicates the remote Guard description (A maximum of 63 characters).