Launching and Customizing the WBM

This chapter describes how to launch and customize the WBM. To access the Cisco Anomaly Guard Module (Guard module) WBM, you must first use the CLI to configure network access for the WBM.

This chapter contains the following sections:

- Configuring Network Access for the WBM
- Launching the WBM
- Configuring the Login Banner
- Configuring the WBM Logo

Configuring Network Access for the WBM

You must use the Guard module CLI to enable the WBM service and to permit network access to the Guard module through the WBM. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For information about accessing and using the Guard module CLI, see the Cisco Anomaly Guard Module Configuration Guide.

To configure network access for the WBM, perform the following steps using the Guard module CLI:

---

**Step 1** Log on to the Guard module CLI using a console or a Secure Shell (SSH) connection.

**Step 2** Enter configuration mode by entering the following command in global mode:
```
admin@GUARD# configure
```

**Step 3** Enable the WBM service by entering the following command:
```
admin@GUARD-conf# service wbm
```

**Step 4** Permit access to the Guard module from the WBM by entering the following command:
```
admin@GUARD-conf# permit wbm ip-addr [ip-mask] [if-service]
```

The `ip-addr` and `ip-mask` arguments define the IP address of the client device that you will use to connect to the WBM.

The optional `if-service` argument specifies the management port designator that restricts user access to the management interface only. The default is all interfaces. Enter `eth1`. 
Chapter 2      Launching  and Customizing the WBM

Launching the WBM

To launch the WBM, perform the following steps:

**Step 1**
Open a web browser and enter the Guard module IP address using Secure HTTP (HTTPS):

```
https://Guard module-ip-address/
```

The `Guard module-ip-address` argument is the management IP address of the Guard module.

The Guard module WBM login window appears.

**Step 2**
Enter your username and password and then click **OK**. The WBM home page appears.

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

Use the Guard module CLI to configure the user authentication methods. For detailed information about accessing and using the Guard module CLI, see the *Cisco Anomaly Guard Module Configuration Guide*.

If you fail to connect to the Guard module, check the following troubleshooting tips:

- Verify that you have entered a valid username and password.
- Verify that you have entered the correct Guard module management IP address and are specifying HTTPS in the URL.
- Check the network connections of both the WBM client and the Guard module.
- Ensure that you can connect to the Guard module from the WBM client using SSH. Connecting using SSH will validate the network connection between the WBM and the Guard module.
- Ensure that you have enabled the WBM service and permitted access to the Guard module from the IP address of the WBM client (see the “Configuring Network Access for the WBM” section for more information).
Configuring the Login Banner

The login banner is the text that appears on the screen before user authentication when you open an SSH session, a console port connection, or a WBM session to the Guard module.

The login banner appears in the following locations:

- CLI—Before the password login prompt.
- WBM—On the right side of the Guard module login window.

You must access the Guard module CLI and use the `login-banner` command in configuration mode to configure the login banner. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For detailed information about configuring and importing a login banner, see the Cisco Anomaly Guard Module Configuration Guide.

Configuring the WBM Logo

You can customize the WBM interface by adding a company logo or any customized logo to the WBM web pages.

The new logo appears in the following places:

- On the Guard module Login page under the Cisco Systems logo.
- On all WBM pages on the right side of the Cisco Systems logo.

You must access the Guard module CLI and use the `copy {ftp | sftp | scp} wbm-logo` command in global mode or configuration mode to configure the WBM logo. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For information about using the CLI to import the WBM logo, see the Cisco Anomaly Guard Module Configuration Guide.