



## WBM Basic Procedures

---

This chapter provides an overview of the Web-Based Management (WBM) basic procedures. It provides an explanation on how to set up the WBM in the Guard and how to connect to the Guard's WBM.

### Setting Up the WBM

Before setting up the Web-Based Management (WBM), some basic configuration of the Guard needs to be performed. The following information, at a minimum, must be known for the Guard to be managed:

- The IP address of the Guard
- 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 Guard

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

## Enable the WBM Service

To enable the Guard web based management service, perform the following from the Guard's command line interface:

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

```
service wbm
```

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

```
admin@GUARD-conf> service wbm
admin@GUARD-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 Guard'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 remote 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@GUARD-conf> permit wbm 10.0.0.192 255.255.255.240
admin@GUARD-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 Remote Manager's Station

To connect to the Guard WBM perform the following:

1. In the remote station, open the browser window.
2. Enter the Guard'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:



*Cisco Guard Web Management*

### System Login

User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="OK"/> <input type="button" value="Clear"/>	

119391

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 Guards'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 Guard User Guide*.

---

**Tip**

---

If you fail to connect to the Guard:

- 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 manager's station and the Guard.
  - 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.
-