



CHAPTER 2

Initializing the Guard

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

This chapter contains the following sections:

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

Using the Command-Line Interface

You can control the Guard functions by using the command-line interface (CLI). The Guard 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, protection, 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 Guard CLI. To obtain a list of commands available for each command mode, enter ? at the system prompt.

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

Table 2-2 Guard 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 Guard. The command prompt is as follows: user@GUARD#
Configuration	Allows you to configure features that affect the Guard operation and have restricted user access. To enter configuration mode, use the configure command in global mode. The command prompt is as follows: user@GUARD-conf#
Interface configuration	Allows you to configure the Guard networking interfaces. To enter interface configuration mode, use the interface command in configuration mode. The command prompt is as follows: user@GUARD-conf-if-<interface-name>#
Router configuration	Allows you to configure the Guard routing configuration. To enter router configuration mode, use the router command in configuration mode. The command prompt is as follows: router>

Table 2-2 Guard Command Configuration Modes (continued)

Mode	Description
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@GUARD-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@GUARD-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@GUARD-conf-zone-<zone-name>-policy-<policy-path>#</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.
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	<p>Enter the more <i>number-of-lines</i> command.</p> <p>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.</p> <p>The <i>number-of-lines</i> argument configures the number of additional lines to be displayed once you press the Spacebar.</p>

Table 2-3 CLI Rules (continued)

Action	Keyboard Sequence
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 / (forward 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 Guard 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 includes the following topics:

- [Using Help](#)
- [Using the 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 the 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 define the direction of the operation. When you enter the keyword before you enter the command, the Guard copies the data from the Guard to the server. When you enter the command before you enter the keyword, the Guard copies the data from the server to the Guard. For example, the **copy log ftp** command copies the log file from the Guard to the FTP server. The **copy ftp new-version** command copies the new software version file from the FTP server to the Guard.

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 **learning policy-construction *** command, the policy construction phase is activated for all the zones that are configured on the Guard.

If you enter the **learning policy-construction scan *** command, the policy construction phase is activated for all the zones that are configured on the Guard 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 Guard for the First Time

This section shows how to establish the initial session with the Guard 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 Guard for the first time, perform the following steps:

-
- Step 1** Press the power control button on the front of the Guard.
After the Guard boot process completes, the software prompts you to enter a username.



Note During power-up, the green power LED on the front of the Guard is on.

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 Enter 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 Guard by entering the following command:

```
configure [terminal]
```

The following example shows how to enter configuration mode:

```
user@GUARD# configure  
user@GUARD-conf#
```

Configuring the Guard Interfaces

The Guard 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 traffic.

The giga0 and giga1 (Gigabit Ethernet) interfaces comprise the in-band NICs that the Guard uses for management and zone traffic. The giga0 and giga1 interfaces provide the physical interface on which virtual interfaces (VLANs and tunnels) are configured. Configuring the Guard interfaces serves as a basis for the traffic diversion procedures. See [Chapter 4, “Configuring Traffic Diversion,”](#) for more information.

You configure a Guard interface by entering the **interface** command and specifying the interface type and number. Many Guard features are enabled on a per-interface basis.

The following guidelines apply to all physical and virtual interface configuration processes:

- Each interface must be configured with an IP address and an IP subnet mask unless you configure IP addresses for individual VLANs.
- 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.

This section contains the following topics:

- [Configuring a Physical Interface](#)

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

Configuring a Physical Interface

Configure a physical interface to connect the Guard to a network. The Guard 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 Guard 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 Guard supports the following interfaces:

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

Step 2 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) For 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
auto	Enables the interface autonegotiation capability. The interface automatically operates at 10/100/1000 Mbps and 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. The default setting is auto .
half	Specifies half-duplex operation.
full	Specifies full-duplex operation.
<i>speed</i>	Interface speed in megabits per second (Mbps). Enter 10 , 100 , or 1000 .

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 Guard for the configuration change to take effect.

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

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

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

Configuring a VLAN

You can define VLANs on the in-band interfaces only.

To define a VLAN on the Guard, perform the following steps:

Step 1 Enter VLAN interface configuration mode, if one exists, or define a new VLAN by entering the following command in configuration mode:

```
interface gigax.vlan-id
```

The *vlan-id* argument is an integer that specifies the VLAN ID number. The VLAN ID is a TAG IEEE 802.1Q number.

The *x* argument specifies the interface. Enter 0 or 1 for the in-band interface.

Step 2 Set the VLAN 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 MTU by entering the following command:

```
mtu integer
```

The *integer* argument is an integer between 576 and 1824 bytes. The default MTU value is 1500 bytes.

Step 4 Activate the interface by entering the following command:

```
no shutdown
```

The following example shows how to configure a VLAN on the Guard:

```
user@GUARD-conf# interface giga1.2
user@GUARD-conf-if-giga1.2# ip address 192.168.5.8 255.255.255.0
user@GUARD-conf-if-giga1.2# no shutdown
```

Configuring a Loopback Interface

You can specify a virtual interface called a loopback interface to emulate a physical interface. You can use the loopback interface to configure advanced traffic diversion configurations, such as the long traffic diversion process.

In applications where other routers or access servers attempt to reach this loopback interface, you must configure a routing protocol to distribute the subnet assigned to the loopback address.

To configure the loopback interface, perform the following steps:

Step 1 Enter the loopback interface configuration mode, if one exists, or define a new loopback interface by entering the following command in configuration mode:

```
interface if-name
```

The *if-name* argument specifies the loopback interface name. The interface name is **lo:***integer* where *integer* is an integer between 0 and 99.

Step 2 Set the loopback 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).

The following example shows how to configure a loopback interface:

```
user@GUARD-conf# interface lo:0
user@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
```

Configuring a Tunnel

You can define a Generic Routing Encapsulation (GRE) or an IP in IP (IPIP) tunnel for the Guard to use in the traffic diversion process.

To define a tunnel, perform the following steps:

- Step 1** Enter the tunnel interface configuration mode, if one exists, or define a new tunnel by entering the following command in configuration mode:

```
interface {greX | ipipY}
```

The *X* argument is an integer between 0 and 1024 bytes assigned to a GRE tunnel.

The *Y* argument is an integer between 0 and 1024 bytes assigned to an IPIP tunnel.

- Step 2** Set the tunnel 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). The default subnet mask is 255.255.255.255.

- Step 3** Set the tunnel source IP address by entering the following command:

```
tunnel source source ip
```

The *source ip* argument specifies the tunnel source IP address. This IP address will be used as the source address for the packets in the tunnel. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).

- Step 4** Set the tunnel destination IP address by entering the following command:

```
tunnel destination destination-ip
```

The *destination ip* argument specifies the tunnel destination IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).

- Step 5** (Optional) Define the interface MTU by entering the following command:

```
mtu integer
```

The *integer* argument is an integer between 576 and 1480. The default value for an IPIP tunnel is 1480 bytes. The default value for a GRE tunnel is 1476 bytes.

- Step 6** Activate the interface. Enter the following command:

```
no shutdown
```

The following example shows how to configure a GRE tunnel:

```
user@GUARD-conf# interface gre2
user@GUARD-conf-if-gre2# ip address 192.168.121.1 255.255.255.0
user@GUARD-conf-if-gre2# tunnel source 192.168.8.8
user@GUARD-conf-if-gre2# tunnel destination 192.168.250.2
user@GUARD-conf-if-gre2# no shutdown
```

Checking the Status of a GRE Tunnel

You can configure the Guard to send keepalive messages over a GRE tunnel at specific times to keep the interface active. You can also specify the number of times that the Guard sends a keepalive packet without receiving a response before the Guard brings the tunnel down.

You configure the keepalive time interval in 1-second increments. If you do not change the retries default value, the Guard declares a GRE tunnel down after 10 consecutive intervals have passed without the Guard receiving a keepalive packet response.

**Caution**

When the Guard declares a GRE tunnel down, the Guard stops using the tunnel for injection. If no other means of traffic injection exist, the Guard suspends zone traffic diversion along with traffic learning or zone protection.

The Guard continues to send keepalive messages even when the GRE tunnel is declared down. If the tunnel end returns the keepalive message, the Guard activates the tunnel and resumes traffic diversion along with zone learning or zone protection.

To enable keepalive messages on a GRE tunnel, use the following command in GRE interface configuration mode:

```
keepalive [refresh-time [retries]]
```

Table 2-5 provides the arguments for the **keepalive** command.

Table 2-5 Arguments for the keepalive Command

Parameter	Description
<i>refresh-time</i>	(Optional) Time interval in seconds at which keepalive messages are sent. Enter an integer from 1 to 32767. The default refresh time is 3 seconds.
<i>retries</i>	(Optional) Number of times that the Guard continues to send keepalive packets without a response before bringing the tunnel interface protocol down. Enter an integer from 1 to 255. The default number of retries is 10.

The following example shows how to enable keepalive messages on a GRE tunnel:

```
user@GUARD-conf-if-gre2# keepalive 60 5
```

Clearing the Counters of a Physical Interface

You can clear the counters of physical interfaces that are used for data (giga1 or giga2) 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 giga1:

```
user@GUARD-conf-if-giga1# clear counters
```

Configuring the Default Gateway

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



Caution

If you do not configure the default gateway IP address, the Guard may not be accessible to the network.

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@GUARD-conf# default-gateway 192.168.100.1
```

Adding a Static Route to the Routing Table

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

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

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

Table 2-6 provides the arguments for the **ip route** command.

Table 2-6 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 a host route IP address. 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).
<i>nexthop-ip</i>	Forwarding or the 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 neighboring router IP address that is directly accessible.

Table 2-6 Arguments for the ip route Command (continued)

Parameter	Description
<i>if-name</i>	(Optional) Interface on the Guard over which the destination is reachable. If you do not specify an interface, the next-hop IP address in the Guard routing table determines the interface used.

The following example shows how to configure a static route:

```
user@GUARD-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.

Configuring the Proxy IP Address

The Guard proxy IP address is required for the proxy mode anti-spoofing protection mechanisms in which the Guard serves as a TCP proxy to the zone. The Guard first authenticates new connections and only then initiates a connection with the zone using its own IP address as the source IP address. You must configure a proxy IP address before activating zone protection.



Caution

You cannot activate zone protection without defining a proxy IP address.

Do not assign the Guard with a proxy IP address while zone protection is enabled.

We recommend that you configure three to four proxy IP addresses if your network uses load balancing to distribute network overload or if your network requires a high number of concurrent connections.

You can configure up to 60 proxy IP addresses; however, we recommend that you do not configure more than 20 proxy IP addresses because more proxy IP addresses consume more memory resources.

To configure a Guard anti-spoofing proxy IP address, use the following command in configuration mode:

```
proxy ip-addr
```

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

You must verify the route between every zone and the Guard proxy IP address. The Guard does not answer ping requests to its proxy IP address.

To configure additional proxy IP addresses, reenter the command.

The following example shows how to configure a proxy IP address:

```
user@GUARD-conf# proxy 192.168.100.34
```

Managing the Guard

Initially, you can manage the Guard 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 Guard. See the [“Assigning Privilege Levels with Passwords”](#) section on page 3-9 for more information.

After you configure the Guard networking (see the “[Configuring the Guard Interfaces](#)” section on page 2-7), you can access and manage the Guard using one of the following methods:

- Access using a Secure Shell (SSH) session.
- Access the Guard using a Web-Based Manager (WBM).
- Access the Guard using the 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 Guard with a Web-Based Manager](#)
- [Managing the Guard with the Cisco DDoS MultiDevice Manager](#)
- [Accessing the Guard with SSH](#)

Managing the Guard with a Web-Based Manager


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

To enable the WBM and manage the Guard, 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 Guard from the remote manager IP address by entering the following command in configuration mode:
- ```
permit wbm { * | ip-addr [ip-mask] }
```

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

Table 2-7 Arguments for the permit wbm Command

Parameter	Description
*	Asterisk wildcard character that allows access by all remote manager IP addresses.
	 Caution For security reasons, we do not recommend that you permit access to a service from all IP addresses.
<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://Guard-ip-address/
```

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

The Guard 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 correctly, the Guard home page displays.

If you have the Guard configured to use Terminal Access Controller Access Control Plus (TACACS+) authentication, the Guard uses the TACACS+ user database for user authentication instead of using its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Guard 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 Guard WBM:

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

For information about using the WBM to manage your Guard, see the appropriate *Cisco Web-Based Manager Configuration Guide*.

Managing the Guard 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 Guards from the web using a web browser. To use the MDM to manage your network of Guards, 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 Guard and permit access by the MDM as described in the following procedure.

To enable the MDM service on the Guard, 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 Guard 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@GUARD-conf# service mdm
user@GUARD-conf# mdm server 192.168.30.32
```

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

Accessing the Guard with SSH

You can access the Guard using a Secure Shell (SSH) connection.

The SSH service is enabled by default.


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

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

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

Table 2-8 provides the arguments for the **permit ssh** command.

Table 2-8 Arguments for the permit ssh Command

Parameter	Description
<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).
*	Asterisk wildcard character that allows access by any remote network.
	 <p>Caution For security reasons, we recommend that you not permit access to all remote networks.</p>

- Step 2** Establish a connection from the remote network address and enter your login username and password. If you have the Guard configured to use TACACS+ authentication, the Guard uses the TACACS+ user database for user authentication instead of using its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Guard 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 Guard to use a locally configured login and password for authentication. See the “[Configuring Authentication](#)” section on page 3-4 for more information.
- Add the remote connection SSH public key to the Guard SSH key list. See the “[Managing SSH Keys](#)” section on page 3-23 for more information.

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

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

