



# CHAPTER 14

## Maintaining Your WAAS System

This chapter describes the tasks you may need to perform to maintain your WAAS system.



### Note

Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

This chapter contains the following topics:

- [Upgrading the WAAS Software, page 14-1](#)
- [Backing Up and Restoring your WAAS System, page 14-9](#)
- [Switching a WAAS Central Manager from Standby to Primary, page 14-20](#)
- [Configuring a Disk Error-Handling Method, page 14-22](#)
- [Activating All Inactive WAAS Devices, page 14-23](#)
- [Rebooting a Device or Device Group, page 14-24](#)
- [Performing a Controlled Shutdown, page 14-24](#)

## Upgrading the WAAS Software

[Table 14-1](#) outlines the steps you must complete to upgrade your WAAS software to a more recent version.

We recommend that all devices in your WAAS network should be running the same version of the WAAS software. If some of your WAAS devices are running different software versions, the WAAS Central Manager should be the lowest version. For details on version interoperability limitations, see the *Release Note for Cisco Wide Area Application Services*.

**Table 14-1** Checklist for Upgrading the WAAS Software

Task	Additional Information and Instructions
1. Determine the current software version running on your WAAS network.	Check the software version that you are currently using so when you go to Cisco.com you know if there is a newer version to download.  For more information, see the <a href="#">“Determining the Current Software Version” section on page 14-2</a> .

Table 14-1 Checklist for Upgrading the WAAS Software (continued)

Task	Additional Information and Instructions
2. Obtain the new WAAS software version from Cisco.com.	Visit Cisco.com to download a newer software version and place this file on a local FTP or HTTP server. For more information, see the “ <a href="#">Obtaining the Latest Software Version from Cisco.com</a> ” section on page 14-2.
3. Register the new software version with the WAAS Central Manager.	Register the URL of the new software file so the WAAS Central Manager knows where to go to access the file. For more information, see the “ <a href="#">Specifying the Location of the Software File in the WAAS Central Manager GUI</a> ” section on page 14-3.
4. Upgrade your WAAS devices using Device Groups.	Upgrade all your WAAS devices (except the WAAS Central Manager) that are members of a device group. For more information, see the “ <a href="#">Upgrading Multiple Devices Using Device Groups</a> ” section on page 14-5.
5. Upgrade your WAAS Central Manager.	After upgrading all your WAAS devices, upgrade the primary and standby WAAS Central Managers. For more information, see the “ <a href="#">Upgrading the WAAS Central Manager</a> ” section on page 14-7.
6. Delete the software version file.	After completely upgrading your WAAS network, you can remove the software file if desired. For more information, see the “ <a href="#">Deleting a Software File</a> ” section on page 14-8.

## Determining the Current Software Version

To view the current software version running on any particular device, choose **Devices > Devices**. The Devices window displays the software version for each device listed.

You can also click the **Edit** icon next to the name of a device in the Devices window. The Device Home window appears, listing the software version for that device.



**Note** The software version is not upgraded until a software upgrade has been successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Alternatively, in the Contents pane for any given device, choose **Monitoring > Show/Clear Commands > Show Commands**. Choose **version** and click **Submit**. A secondary window pops up and displays the CLI output for the **show version** command.

## Obtaining the Latest Software Version from Cisco.com

To obtain the latest WAAS software version from Cisco.com, follow these steps:

- Step 1** Launch your preferred web browser and open this location:  
<http://www.cisco.com/kobayashi/sw-center/sw-content.shtml>

- Step 2** When prompted, log in to Cisco.com using your designated username and password. The Content Networking window appears, listing the available software products.
- Step 3** Choose a link to the content networking software product that you want. The Software Download window appears.
- Step 4** Click the **Download WAAS Software images (contains strong encryption)** link.  
The Content Networking window for Cisco WAAS Software appears.
- Step 5** Click the link to the WAAS cryptographic software release that you want.  
The window refreshes, listing all the software files (and meta files) available for that release.
- Step 6** Locate the software file that you want to download by consulting the Release column for the proper release version of the software.  
The software files will have names similar to the following: WAAS-4.0.0-K9.bin
- Step 7** Click the link for the software file that you want to download.  
The Enter Network Password dialog box appears. Enter your username and password, click **OK**, and proceed as follows:
- If this is the first time you have downloaded a software file from Cisco.com, the Encryption Software Export Distribution Authorization form appears.
    - Fill out the form and click **Submit**. The Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy appears.
    - Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.
  - If you previously filled out the Encryption Software Export Distribution Authorization form and read and accepted the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again. Instead, the Encryption Software Export/Distribution Form appears after you click **OK** in the Enter Network Password dialog box.
- Step 8** Read the Encryption Software Export/Distribution Form, click the **Yes** or **No** radio button, and click **Submit**. A security alert dialog box pops up.
- Step 9** Click **Yes** in the Security Alert dialog box. The Software Download window reappears.
- Step 10** Right-click the software file link to download the software and use the **Save Link As** or the **Save Link Target As** option to save the file to your FTP or HTTP server.
- Step 11** Register the location of the software file in the WAAS Central Manager GUI, as described in the section that follows.
- 

## Specifying the Location of the Software File in the WAAS Central Manager GUI

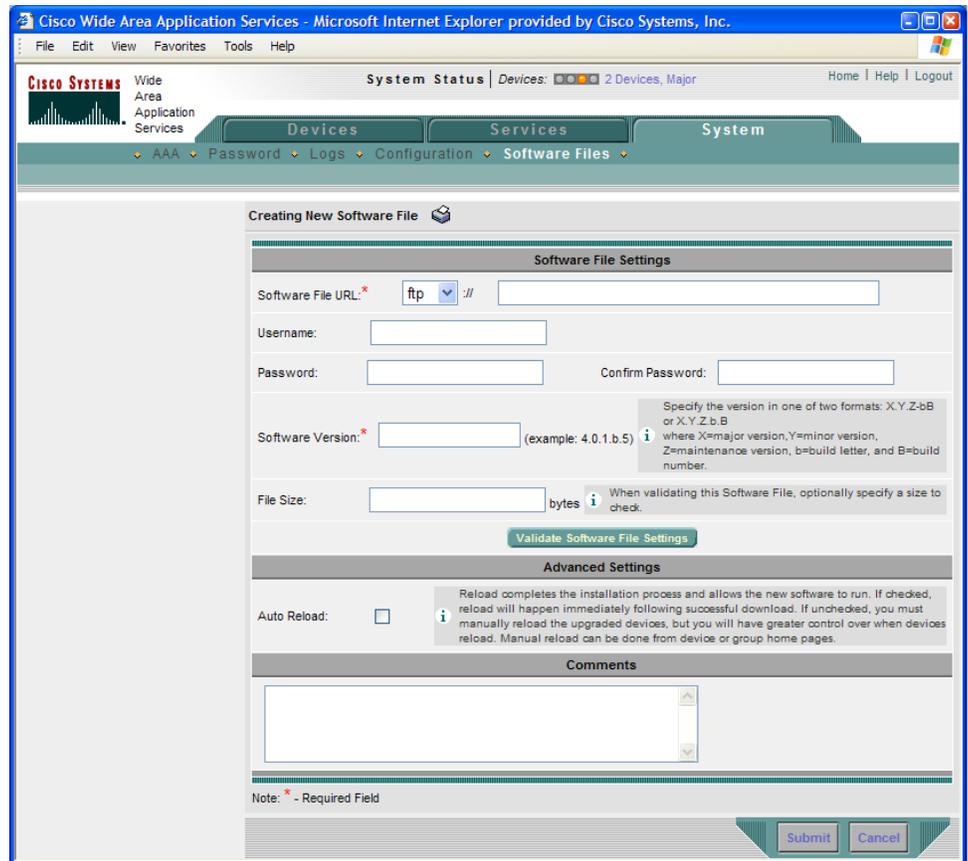
To upgrade your WAAS software, you must first specify the location of the WAAS software file in the WAAS Central Manager GUI and configure the software file settings. The software file settings form in the WAAS Central Manager GUI defines the software file (.bin) and can be used to specify how to obtain the software file, and whether to preposition it or download it directly to a device.

To configure the software file settings form, follow these steps:

- 
- Step 1** From the WAAS Central Manager GUI, choose **System > Software Files**.
- Step 2** Click the **Create New Software File** icon in the taskbar.

The Creating New Software File window appears. (See Figure 14-1.)

**Figure 14-1** Creating New Software File Window



- Step 3** In the Software File URL field, specify the location of the new WAAS software file as follows:
- Choose a protocol (**http** or **ftp**) from the drop-down list.
  - Enter the URL for the .bin software file that you downloaded from Cisco.com. For example, a valid URL might look like the following:  

```
http://internal.mysite.com/waas/WAAS-4.x.x-K9.bin
```

 where *WAAS-4.x.x-K9* is the name of the software upgrade file. (The filename might include the version number.)
- Step 4** If your server requires user login authentication, enter your username in the Username field and enter your login password in the Password field. Enter the same password in the Confirm Password field.
- Step 5** Enter the software version number in the Software Version field.  
 You can copy this number from the version portion of the software filename in the software file URL. Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B, where X = major version, Y = minor version, Z = maintenance version, b = build letter, and B = build number.
- Step 6** If you want the size of the software file considered during validation, enter a file size (in bytes) in the File Size field.  
 If you leave this field blank, the URL is checked without regard to the software file size.

**Step 7** Click the **Validate Software File Settings** button to validate the Software File URL, Username, and Password fields.

When you click the **Validate Software File Settings** button, the following occurs:

- The software file URL is resolved.
- A connection to the software file URL is established using the username and password, if specified.
- If a file size is specified, the actual size of the software file is obtained and compared against the value in the File Size field.
- A message is returned, indicating success or errors encountered.

**Step 8** In the Advanced Settings section, check the **Auto Reload** check box to automatically reload a device when you upgrade the software. If you do not check this box, you will need to manually reload a device after you upgrade the software on it, to complete the upgrade process.

**Step 9** (Optional) Enter comments in the field provided.

**Step 10** Click **Submit**.

A message appears indicating that the upgrade is successful. Click **OK**.



**Caution**

If your browser is configured to save the username and password for the WAAS Central Manager GUI, the browser will autopopulate the username and password fields in the Creating New Software File window. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the WAAS Central Manager. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the Update Software window.

To reload a device from the CLI, use the **reload EXEC** command.

## Upgrading Multiple Devices Using Device Groups



**Note**

This procedure is for WAE devices only. WAAS Central Manager devices cannot be upgraded using device groups.

To upgrade to a more recent WAAS software release on multiple devices, follow these steps:

**Step 1** From the WAAS Central Manager GUI, choose **Devices > Device Groups**.

The Device Groups listing window appears, listing all the device groups in your WAAS network.

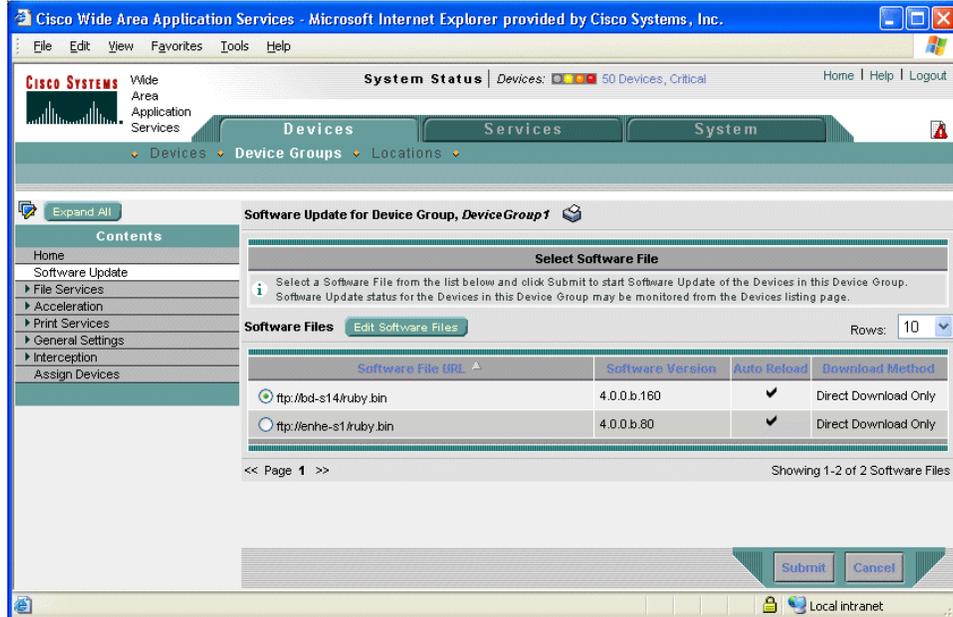
**Step 2** Click the **Edit** icon next to the name of the device group that you want to upgrade.

The Modifying Device Group window appears.

**Step 3** In the Contents pane, choose **Software Update**.

The Software Update for Device Group window appears. (See [Figure 14-2](#).)

Figure 14-2 Software Update for Device Group Window



- Step 4** Choose the software file URL from the Software File URL list by clicking the radio button next to the filename.



**Note** If the software file URL is not displayed, click **Edit Software Files**. This button brings you to the System > Software Files window where you can specify the location of the software file as described in the “[Specifying the Location of the Software File in the WAAS Central Manager GUI](#)” section on page 14-3.

- Step 5** Click **Submit**.

To view the progress of an upgrade, go to the Devices window (**Devices > Devices**) and view the software upgrade status message in the Software Version column. These intermediate messages are also written to the system log on WAAS devices. See [Table 14-2](#) for a description of the upgrade status messages.

**Table 14-2** Upgrade Status Messages

Upgrade Status Message	Condition
Pending	The request has yet to be sent from the WAAS Central Manager to the device, or receipt of the request has yet to be acknowledged by the device.
Downloading	The download method for the software file is being determined.
Proceeding with Download	The download method for the software file is determined to be direct download. Proceeding with the request for direct download of the software file.
Download in Progress (Completed ...)	Direct download of the software file is being processed. "Completed" indicates the number of megabytes processed.
Download Successful	The direct download of the software file has been successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log.
Proceeding with Flash Write	A request has been made to write the software file to the device flash memory.
Flash Write in Progress (Completed ...)	The write of the device flash memory is being processed. "Completed" indicates the number of megabytes processed.
Flash Write Successful	The flash write of the software file has been successful.
Reloading	A request to reload the device has been made in order to complete the software upgrade. The device may be offline for several minutes.
Reload Needed	A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.
Cancelled	The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the CLI.
Update Failed	The software upgrade could not be completed. Troubleshooting is required; see the device system message log.

## Upgrading the WAAS Central Manager

When upgrading software in your WAAS network, begin with WAE devices before upgrading the WAAS Central Manager. The WAAS Central Manager may reboot at the conclusion of the upgrade procedure (if Auto Reload was checked in the Creating New Software File window), causing you to temporarily lose contact with the device and the graphical user interface. After the WAAS Central Manager has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the WAAS software.

Primary and standby WAAS Central Manager devices must be running the same version of WAAS software. If they are not, the standby WAAS Central Manager detects this and will not process any configuration updates it receives from the primary WAAS Central Manager. If you use the primary WAAS Central Manager to perform the software upgrade, you need to upgrade your standby WAAS Central Manager first, then upgrade your primary WAAS Central Manager. We also recommend that you create a database backup for the primary WAAS Central Manager and copy the database backup file to a safe place before you upgrade the software.

Use this upgrade procedure for WAAS Central Manager devices. You can also use this upgrade procedure to upgrade WAAS devices one-at-a-time.

To upgrade your software to another WAAS software release on a single device, follow these steps:

- 
- Step 1** From the WAAS Central Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon of the device that you want to upgrade.  
The Device Home window appears.
- Step 3** Verify that the device is not already running the version that you plan to upgrade to.
- Step 4** Click the **Update Software** button.  
The Software Update window appears.
- Step 5** Choose the software file URL from the Software Files list by clicking the radio button next to the filename.
- 
-  **Note** If the software file URL is not displayed, click **Edit Software Files**. This button brings you to the System > Software Files window where you can specify the location of the software file as described in the [“Specifying the Location of the Software File in the WAAS Central Manager GUI”](#) section on page 14-3.
- 
- Step 6** Click **Submit**, and then click **OK** to confirm your decision.  
The Devices listing window reappears. You can monitor the progress of your upgrade from this window. Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the WAAS devices. See [Table 14-2](#) for a description of upgrade status messages.
- 

## Deleting a Software File

After you have successfully upgraded your WAAS devices, you can remove the software file from your WAAS system.



**Note** You may want to wait a few days before removing a software file in the event you need to downgrade your system for any reason.

---

To delete a WAAS software file, follow these steps:

- 
- Step 1** From the WAAS Central Manager GUI, choose **System > Software Files**.
- Step 2** Click the **Edit** icon next to the software file that you want to delete. The Modifying Software File window appears.
- Step 3** Click the **Trash** icon in the taskbar.  
You are prompted to confirm your decision to delete the software file.
- Step 4** Click **OK**.  
You are returned to the Software Files listing window with the selected software file removed from the WAAS network.
- 

## Backing Up and Restoring your WAAS System

This section contains the following topics:

- [Backing Up and Restoring the WAAS Central Manager Database, page 14-9](#)
- [Backing Up and Restoring a WAE Device, page 14-11](#)
- [Using the Cisco WAAS Software Recovery CD-ROM, page 14-12](#)
- [Recovering the System Software, page 14-15](#)
- [Recovering a Lost Administrator Password, page 14-17](#)
- [Recovering from Missing Disk-Based Software, page 14-18](#)
- [Recovering WAAS Device Registration Information, page 14-19](#)

## Backing Up and Restoring the WAAS Central Manager Database

The WAAS Central Manager device stores WAAS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS database contents for greater system reliability.

The CMS database backup is in a proprietary format that contains an archive database dump, WAAS Central Manager registration information, and device information that the WAAS Central Manager uses to communicate with other WAAS devices. CMS database backup files are not interchangeable between primary and standby WAAS Central Manager devices. This means you cannot use the backup file from a primary WAAS Central Manager to restore a standby WAAS Central Manager.

To back up the CMS database for the WAAS Central Manager, use the **cms database backup EXEC** command. For database backups, you need to specify the location, password, and user ID of the remote server that you want to store the backup file.



### Note

The CMS database backup does not backup print drivers. When you perform a Central Manager database backup, you must reinstall your print drivers.

---

To back up and restore the CMS database, follow these steps:

- Step 1** On the WAAS Central Manager GUI device, use the **cms database backup** command to back up the CMS database to a file, as shown in the following example:

```
CDM# cms database backup
creating backup file with label 'backup'
backup file local1/waas-db-7-22-2006-17-36.dump is ready. use 'copy' commands to move the
backup file to a remote host.
```



**Note** The backup file is automatically given a name in the following format `cms-db-date-timestamp.dump`. For example, `cms-db-7-22-2006-17-36.dump`. Note that the timestamp is in 24-hour format (HH:MM) that does not show seconds.

- Step 2** Save the file to a remote server by using the **copy disk ftp** command.

This command copies the file from the local disk to a remote FTP server, as shown in the following example:

```
CDM# cd /local1
CDM# copy disk ftp 10.86.32.82 /incoming waas-db-7-22-2006-17-36.dump
waas-db-7-22-2006-17-36.dump

Enter username for remote ftp server:ftp
Enter password for remote ftp server:*****
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-2.6.1-18) ready.
Password required for ftp.
Sending:PASS *****
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending:CWD /incoming
CWD command successful.
Sending PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending:STOR acns-db-9-22-2002-17-36.dump
Opening BINARY mode data connection for waas-db-7-22-2006-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

- Step 3** Restore the CMS database as follows:

- a. Disable the CMS service.

```
CDM# no cms enable
```



**Note** Stopping the CMS service disables the WAAS Central Manager GUI. All users currently logged into this GUI are automatically logged out once the CMS service is disabled.

- b. Delete the existing CMS database.

```
CDM# cms database delete
```

- c. Restore the CMS database contents from the backup file.

```
CDM# cms database restore waas-db-7-22-2006-17-36.dump
```

- d. Enable the CMS service.

```
CDM# cms enable
```

---

## Backing Up and Restoring a WAE Device

We recommend that you back up the database of each WAAS device on a regular basis in case a system failure should occur.



### Note

The backup and restore methods described in this section only apply to a WAE device that is not configured as a WAAS Central Manager. For information on backing up the WAAS Central Manager device, see the [“Backing Up and Restoring the WAAS Central Manager Database” section on page 14-9](#).

You can use either of the following methods to back up and restore the database of an individual WAE device:

- WAE Device Manager—For information on using the WAE Device Manager to back up and restore a device’s database, see the [“Backing Up the Configuration Files” section on page 10-8](#).
- CLI—You can use the following commands to back up and restore a device’s database:
  - **wafs backup-config**—Saves the entire WAFS system configuration to a file, including configuration for file servers, printers, and users. We strongly recommend that you register your WAE again after you use this command.
  - **wafs restore-config**—Restores configuration based on the specified backup file. This command automatically performs a reload function.
  - **copy running-config**—Saves the currently running network configuration to the startup configuration.

Additionally, you can restore a WAE to the default configuration that it was manufactured with at any time by removing the user data from the disk and Flash memory, and erasing all existing files cached on the appliance. Basic configuration information, such as network settings, can be preserved. The appliance is accessible through Telnet and Secure Shell (SSH) after it reboots.



### Note

If software upgrades have been applied, the restoration process returns to the defaults of the currently installed version and not the factory defaults.

To restore a WAE to its factory defaults or the defaults of the current configuration from the CLI, use the **restore factory-default [preserve basic-config] EXEC** command.

For more information about the CLI commands, see the *Cisco Wide Area Application Services Command Reference*.

## Using the Cisco WAAS Software Recovery CD-ROM

A software recovery CD-ROM ships with WAE hardware devices. This section contains instructions for using the software recovery CD-ROM to reinstall your system software if for some reason the software that is installed has failed.



### Caution

If you upgraded your software after you received your software recovery CD-ROM, using the CD-ROM software images may downgrade your system.

Cisco WAAS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All of these components must be correctly installed for Cisco WAAS software to work properly.

The software is contained in two types of software images provided by Cisco Systems:

- A .bin image containing disk and flash memory components
- A .sysimg image containing a flash memory component only

An installation containing only the WAAS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

The .sysimg component is provided for recovery purposes, and allows for repair of flash memory only without modifying the disk contents.

The options described in the following sections are available from the software recovery CD-ROM installer menu:

- **Option 1: Configure Network**—If the .bin image you need to install is located on the network instead of the CD-ROM (which may be the case when an older CD-ROM is used to install new software), then you must choose this option to configure the network before attempting to install the .bin image.

This option is automatically performed if you install a .sysimg file from the network.

- **Option 2: Manufacture Flash**—This option verifies the flash memory and, if invalid, automatically reformats it to contain a Cisco standard layout. If reformatting is required, a new cookie is automatically installed.

This option is automatically performed as part of a .bin or .sysimg installation.

- **Option 3: Install Flash Cookie**—This option generates a hardware-specific platform cookie and installs it in flash memory. This option only needs to be performed if there has been a change in the hardware components, such as replacing the motherboard, or moving a flash memory card between systems.

This option is automatically performed during the flash manufacturing process, if needed, as part of a .bin or .sysimg installation.

- **Option 4: Install Flash Image from Network and Option 5: Install Flash Image from CD-ROM**—These options allow installation of the flash memory .sysimg only, and do not modify disk contents. They may be used when a new chassis has been provided and populated with the customer's old disks that need to be preserved.

These options automatically perform flash verification and hardware cookie installation, if required. When installing from the network, you are prompted to configure the network if you have not already done so.

- **Option 6: Install Flash Image from Disk**—This option is reserved for future expansion and is not available.
- **Option 7: Wipe Out Disks and Install .bin Image**—This option provides the preferred procedure for installing the Cisco WAAS software.



**Caution** Option 7 erases the content from all disk drives in your device.

This option performs the following steps:

- Checks that flash memory is formatted to Cisco specifications. If yes, the system continues to step b. If no, the system reformats the flash memory, which installs the Cisco file system, and generates and installs a platform-specific cookie for the hardware.
  - Erases data from all drives.
  - Remanufactures the default Cisco file system layout on the disk.
  - Installs the flash memory component from the .bin image.
  - Installs the disk component from the .bin image.
- **Option 8: Exit and Reboot**—This option reboots the device. Remove the CD-ROM before rebooting in order to boot from flash memory.

To reinstall the system software on a WAE appliance using the software recovery CD-ROM, follow these steps:

**Step 1** Connect a serial console to the WAE appliance to be upgraded and use the console for the following steps.

**Step 2** Insert the WAAS 4.0.x CD-ROM in the CD drive of the WAE device.

**Step 3** Reboot the WAE. After the WAE boots, you see the following menu:

```
Installer Main Menu:
 1. Configure Network
 2. Manufacture flash
 3. Install flash cookie
 4. Install flash image from network
 5. Install flash image from cdrom
 6. Install flash image from disk
 7. Wipe out disks and install .bin image
 8. Exit (and reboot)
Choice [0]:
```

**Step 4** Choose option 2 to prepare the flash memory.

This step prepares a cookie for the device and also retrieves the network configuration that was being used by the WAAS software. This network configuration is stored in the flash memory and is used to configure the network when the WAAS software boots up after installation.

**Step 5** Choose option 3 to install the flash cookie that you prepared in the previous step.

**Step 6** Choose option 5 to install the flash image from the CD-ROM.

**Step 7** Choose option 7 to wipe the disks and install the binary image.

This step prepares the disks by erasing them. The WAAS 4.0.x image is installed.

**Step 8** Remove the CD-ROM from the drive.

**Step 9** Choose option 8 to reboot the WAE.

After the WAE reboots, it is running the WAAS 4.0.x software. The WAE has a minimal network configuration and is accessible via the terminal console for further configuration.

To reinstall the system software on an NME-WAE network module installed in a Cisco access router, follow these steps:

**Step 1** Log in to the Cisco router in which the NME-WAE module is installed, and reload the NME-WAE module:

```
router-2851> enable
router-2851# service-module integrated-Service-Engine 1/0 reload
```

**Step 2** Immediately open a session on the module:

```
router-2851# service-module integrated-Service-Engine 1/0 session
```

**Step 3** While the module is reloading, you will see the following option during boot phase 3. Enter \*\*\* as instructed:

```
[BOOT-PHASE3]: enter `***' for rescue image: ***
```

**Step 4** The rescue image dialog appears. The following example demonstrates how to interact with the rescue dialog (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you install a new system image onto your system's boot flash
device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
```

To download an image from network, this software will request the following information from you:

- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username and password on FTP server
- path to system image on server

Please enter an interface from the following list:

- 0: GigabitEthernet 1/0
- 1: GigabitEthernet 2/0

enter choice: **0**

Using interface GigabitEthernet 1/0

Please enter the local IP address to use for this interface:

[Enter IP Address]: **10.1.13.2**

Please enter the netmask for this interface:

[Enter Netmask]: **255.255.255.240**

Please enter the IP address for the default gateway:

[Enter Gateway IP Address]: **10.1.13.1**

Please enter the IP address for the FTP server where you wish to obtain the new system image:

```

[Enter Server IP Address]: 10.107.193.240

Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: username

Please enter the password for username 'username' on FTP server:

Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /

Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: WAAS-4.0.7-K9.sysimg

Here is the configuration you have entered:

Current config:
    IP Address: 10.1.13.2
    Netmask: 255.255.255.240
    Gateway Address: 10.1.13.1
    Server Address: 10.107.193.240
    Username: username
    Password: *****
    Image directory: /
    Image filename: WAAS-4.0.7-K9.sysimg

Attempting download...
Downloaded 15821824 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
..... done.
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.

```

**Step 5** After the module reboots, install the .bin image from an HTTP server:

```
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-4.0.7-k9.bin
```

**Step 6** Reload the module:

```
NM-WAE-1# reload
```

After the module reboots, it is running the WAAS 4.0.x software.

## Recovering the System Software

WAAS devices have a resident rescue system image that is invoked if the image in flash memory is corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can download a system image to the main memory of the device and write it to flash memory.

To install a new system image using the rescue image, follow these steps:

- 
- Step 1** Download the system image file (\*.sysimg) to a host that is running an FTP server.
  - Step 2** Establish a console connection to the device and open a terminal session.
  - Step 3** Reboot the device by toggling the power on/off switch.

The rescue image dialog appears. The following example demonstrates how to interact with the rescue dialog (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
```

```
To download an image, this software will request the following
information from you:
```

- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- server IP address
- which protocol to use to connect to server
- username/password (if applicable)
- path to system image on server

```
Please enter an interface from the following list:
```

```
0: FastEthernet 0/0
1: FastEthernet 0/1
0
```

```
Using interface FastEthernet 0/0
```

```
Please enter the local IP address to use for this interface:
```

```
[Enter IP Address]: 172.16.22.22
```

```
Please enter the netmask for this interface:
```

```
[Enter Netmask]: 255.255.255.224
```

```
Please enter the IP address for the default gateway:
```

```
[Enter Gateway IP Address]: 172.16.22.1
```

```
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
```

```
[Enter Server IP Address]: 172.16.10.10
```

```
Please enter your username on the FTP server (or 'anonymous'):
```

```
[Enter Username on server (e.g. anonymous)]: anonymous
```

```
Please enter the password for username 'anonymous' on FTP server (an email address):
```

```
Please enter the directory containing the image file on the FTP server:
```

```
[Enter Directory on server (e.g. /)]: /
```

```
Please enter the file name of the system image file on the FTP server:
```

```
[Enter Filename on server]: WAAS-4.0.0-K9.sysimg
```

```
Here is the configuration you have entered:
```

```
Current config:
```

```
IP Address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
```

```

Username: anonymous
Password:
Image directory: /
Image filename: WAAS-4.0.0-K9.sysimg

Attempting download...
Downloaded 10711040 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.....Finished
writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
Initializing memory. Please wait.
```

- Step 4** Log in to the device as username **admin**. Verify that you are running the correct version by entering the **show version** command.

```

Username: admin
Password:

Console> enable
Console# show version
Wide Area Application Services (WAAS)
Copyright (c) 1999-2006 by Cisco Systems, Inc.
Wide Area Application Services Release 4.0.0
Version: ce507-5.2.0

Compiled 02:34:38 May 8 2006 by (cisco)
Compile Time Options: PP SS

System was restarted on Thu June 22 16:03:51 2006.
The system has been up for 4 weeks, 1 day, 6 hours, 7 minutes, 23 seconds.
```

## Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, you will need to reset the password on the device.



### Note

There is no way to restore a lost administrator password. You must reset the password to a new one, as described in this procedure.

To reset the password, follow these steps:

- Step 1** Establish a console connection to the device and open a terminal session.

- Step 2** Reboot the device.

While the device is rebooting, watch for the following prompt, then press **Enter** when you see it:

```
Cisco WAAS boot:hit RETURN to set boot flags:0009
```

**Step 3** When prompted to enter bootflags, enter the following value: **0x8000**

For example:

```
Available boot flags (enter the sum of the desired flags):
0x4000 - bypass nvram config
0x8000 - disable login security
```

```
[CE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes
```

[Display output omitted]  
Setting the configuration flags to **0x8000** lets you into the system, bypassing all security. Setting the configuration flags field to **0x4000** lets you bypass the NVRAM configuration.

**Step 4** When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).

```
Cisco WAE Console
```

```
Username: admin
```

**Step 5** When you see the CLI prompt, set the password for the user using the **username password** command in global configuration mode.

```
WAE# configure
WAE(config)# username admin password 0 password
```

You can specify that the password be either clear text or encrypted.




---

**Note** Do not set the user ID (uid).

---

**Step 6** Save the configuration change by using the **write memory** command in EXEC mode.

```
WAE(config)# exit
WAE# write memory
```

**Step 7** (Optional) Reboot your device by using the **reload** command.

```
WAE# reload
```

Rebooting is optional; however, you might want to reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.




---

**Note** In WAAS software, the bootflags are reset to 0x0 on every reboot.

---

## Recovering from Missing Disk-Based Software

Use the procedures in this section to recover from the following types of disk drive issues:

- Your WAAS device contains a single disk drive that needs to be replaced due to a disk failure.

- Your WAAS device contains two disk drives and you intentionally deleted the disk partitions on both drives (diks00 and disk01).

Systems with two or more disk drives are normally protected automatically by RAID-1 on critical system partitions, so the procedures in this section do not need to be followed when replacing a disk drive in a multi-drive system.

To recover from this condition, follow these steps:

- 
- Step 1** Deactivate the device by completing the following steps:
- a. From the WAAS Central Manager GUI, go to **Devices > Devices**.
  - b. Click the **Edit** icon next to the device that you want to deactivate.
  - c. Click **Show Advanced** to display all menu items in the Contents pane.
  - d. From the Contents pane, choose **Activation**. You may need to click **Show Advanced** to display this menu item.  
The Device Activation window appears.
  - e. Uncheck the **Activate** check box, then click **Submit**.  
The device is deactivated.
- Step 2** Power down the device and replace the failed hard drive.
- Step 3** Power on the device.
- Step 4** Install the WAAS software. For more information, see the *Cisco Wide Area Application Services Quick Configuration Guide*.
- Step 5** Use the CMS identity recovery procedure to recover device CMS identity and associate this device with the existing device record on the WAAS Central Manager. For more information, see the [“Recovering WAAS Device Registration Information” section on page 14-19](#).
- 

## Recovering WAAS Device Registration Information

Device registration information is stored both on the device itself and on the WAAS Central Manager. If a device loses its registration identity or needs to be replaced because of a hardware failure, the WAAS network administrator can issue a CLI command to recover the lost information, or in the case of adding a new device, assume the identity of the failed device.

To recover lost registration information, or to replace a failed device with a new one having the same registration information, follow these steps:

- 
- Step 1** Mark the failed device as “Inactive” and “Replaceable” by completing the following steps:
- a. From the WAAS Central Manager GUI, choose **Devices > Devices**.
  - b. Click the **Edit** icon next to the device that you want to deactivate. The Device Home window appears.
  - c. Click **Show Advanced** to display all menu items in the Contents pane.
  - d. In the Contents pane, choose **Activation**. You may need to click **Show Advanced** for this menu item to be displayed.

- e. Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.
- f. Check the **Replaceable** check box, and click **Submit**.




---

**Note** This check box only appears in the GUI when the device is inactive.

---

**Step 2** Configure a system device recovery key as follows:

- a. From the WAAS Central Manager GUI, choose **System > Configuration**.
- b. Click the **Edit** icon next to the System.device.recovery.key property. The Modifying Config Property window appears.
- c. Enter a password in the Value field, and click **Submit**. The default password is **default**.

**Step 3** Configure the basic network settings for the new device.

**Step 4** Open a Telnet session to the device CLI and enter the **cms recover identity keyword EXEC** command. *keyword* is the device recovery key that you configured in the WAAS Central Manager GUI.

When the WAAS Central Manager receives the recovery request from the WAAS device, it searches its database for the device record that meets the following criteria:

- The record is inactive and replaceable.
- The record has the same hostname or primary IP address as given in the recovery request.

If the recovery request matches the device record, then the WAAS Central Manager updates the existing record and sends the requesting device a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the WAAS device receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

**Step 5** Activate the device by completing the following steps:

- a. From the WAAS Central Manager GUI, choose **Devices > Devices**.
  - b. Click the **Edit** icon next to the WAAS device that you want to activate. The Device Home window appears.
  - c. Click **Show Advanced** to display all menu items in the Contents pane.
  - d. In the Contents pane, choose **Activation**. The WAAS device status should be Online.
  - e. Check the **Activate** check box, and click **Submit**.
- 

## Switching a WAAS Central Manager from Standby to Primary

The Cisco WAAS software implements a standby WAAS Central Manager. This process allows you to maintain a copy of the WAAS network configuration on a second WAAS Central Manager device. If the primary WAAS Central Manager fails, the standby can be used to replace the primary.

For interoperability, when a standby WAAS Central Manager is used, it must be at the same software version as the primary WAAS Central Manager to maintain the full WAAS Central Manager configuration. Otherwise, the standby WAAS Central Manager detects this status and does not process any configuration updates that it receives from the primary WAAS Central Manager until the problem is corrected.

**Note**

Before you configure a standby Central Manager, you must manually install your print drivers. Print drivers are not automatically replicated from the primary Central Manager database to the standby device.

If your primary WAAS Central Manager becomes inoperable, you can manually reconfigure one of your warm standby WAAS Central Managers to be the primary WAAS Central Manager. Configure the new role by using the global configuration **central-manager role primary** command as follows:

```
WAE# configure
WAE(config)# central-manager role primary
```

This command changes the role from standby to primary and restarts the management service to recognize the change.

If you switch a warm standby WAAS Central Manager to primary while your primary WAAS Central Manager is still online and active, both WAAS Central Managers detect each other, automatically shut themselves down, and disable management services. The WAAS Central Managers are switched to halted, which is automatically saved in flash memory.

To return halted WAAS Central Managers to an online status, decide which Central Manager should be the primary device and which should be the standby device. On the primary device, execute the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role primary
WAE(config)# cms enable
```

On the standby device, execute the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role standby
WAE(config)# central-manager address primary-CM-ip
WAE(config)# cms enable
```

**Caution**

When you switch a WAAS Central Manager from primary to standby, the configuration on the Central Manager is erased. The Central Manager, after becoming a standby, will begin replicating its configuration information from whichever Central Manager is now the primary. If standby and primary units are not synchronized before switching roles, important configuration information can be lost.

Before you switch Central Manager roles, follow these steps:

- Step 1** Make sure that your Central Manager devices are running the same version of WAAS software.
- Step 2** Synchronize the physical clocks on both devices so that both WAAS Central Managers have the same Coordinated Universal Time (UTC) configured.
- Step 3** Make sure that the standby is synchronized with the primary by checking the status of the following items:
  - a. Check the online status of your devices.

The original standby Central Manager and all currently active devices should be showing as online in the Central Manager GUI. This step ensures that all other devices know about both Central Managers.
  - b. Check the status of recent updates from the primary WAAS Central Manager.

Use the **show cms info EXEC** command and check the time of the last update. To be current, the value of the Time of last config-sync field should be between 1 and 5 minutes old. You are verifying that the standby WAAS Central Manager has fully replicated the primary WAAS Central Manager configuration.

If the update time is not current, determine whether or not there is a connectivity problem or if the primary WAAS Central Manager is down. Fix the problem, if necessary, and wait until the configuration has replicated, as indicated by the time of the last update.

**Step 4** Switch roles in the following order:

a. Switch the original primary to standby mode, as follows:

```
WAE1# configure
WAE1(config)# central-manager role standby
WAE(config)# cms enable
```

b. Switch the original standby to primary mode, as follows:

```
WAE2# configure
WAE2(config)# central-manager role primary
WAE(config)# cms enable
```

The CMS service is restarted automatically when you configure a role change.

## Configuring a Disk Error-Handling Method

The WAAS software allows you to configure how disk errors should be handled and to define a disk device error-handling threshold.

If the bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, then the WAAS software marks the disk drive “bad” and the WAAS device is automatically reloaded. After the WAAS device is reloaded, a syslog message and an SNMP trap are generated.

The disk error-handling threshold option determines how many disk errors can be detected before the disk drive is automatically marked “bad.” By default, this threshold is set to 10. To change the default threshold, use the **disk error-handling threshold** global configuration command. Specify **0** if you never want the disk drive to be marked “bad.”

In the following example, five disk drive errors for a particular disk drive (for example, disk00) will be allowed before the disk drive is automatically marked “bad”:

```
WAE(config)# disk error-handling threshold 5
```

To configure a disk error-handling method using the WAAS Central Manager GUI, follow these steps:

- Step 1** From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.
- Step 2** Click the **Edit** icon next to the device (or device group) for which you want to configure the disk error handling method.
- Step 3** Click **Show Advanced** to display all menu items in the Contents pane.
- Step 4** In the Contents pane, choose **General Settings > Storage > Disk Error Handling**.  
The Disk Error Handling Settings window appears.

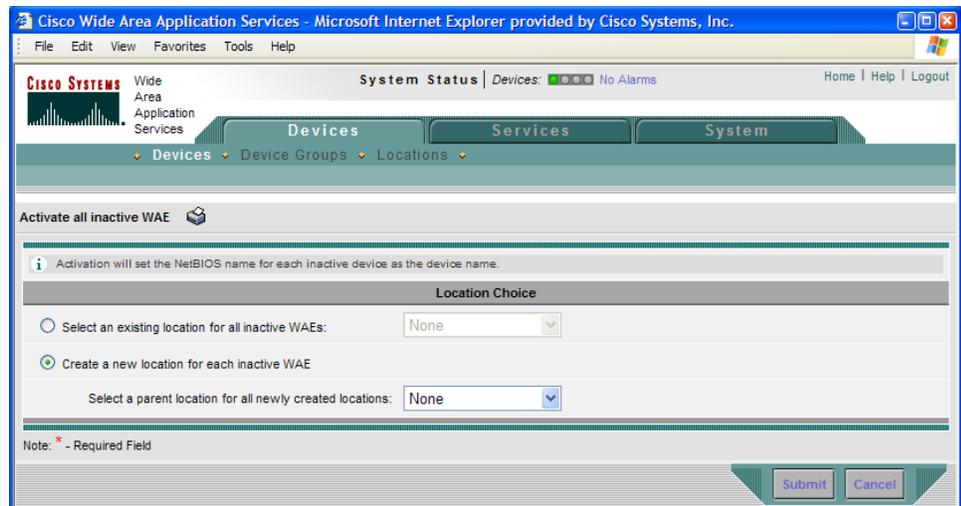
- Step 5** Check the **Enable** check box to enable the window for configuration, and then check the following options as necessary:
- **Enable Disk Error Handling Reload**—Forces the device to reload the disk if the file system (sysfs) (disk00) has problems. This option is disabled by default.
  - **Enable Disk Error Handling Remap**—Forces the disks to attempt to remap disk errors automatically. This option is enabled by default.
  - **Enable Disk Error Handling Threshold**—Specifies the number of disk errors allowed before the disk is marked as bad. You must enter a number between 0 to 100 in the Threshold field. The default threshold is 10. This option is disabled by default.
- Step 6** Click **Submit** to save the settings.

## Activating All Inactive WAAS Devices

To activate all inactivated WAAS devices in your network, follow these steps:

- Step 1** From the WAAS Central Manager GUI, choose **Devices > Devices**. The Devices listing window appears.
- Step 2** Click the **Activate all inactive WAEs** icon in the taskbar. The Activate All Inactive WAEs window appears. (See [Figure 14-3](#).)

**Figure 14-3** Activating Inactive Devices



- Step 3** Choose an existing location for all inactivated WAAS devices by clicking the **Select an existing location for all inactive WAEs** radio button, and then choose a location from the drop-down list.
- Alternatively, choose to create a new location for each inactive device by clicking the **Create a new location for each inactive WAE** radio button. Specify a parent location for all newly created locations by choosing a location from the Select a parent location for all newly created locations drop-down list.

- Step 4** Click **Submit**. The inactive WAEs are reactivated and placed in the specified location.
- 

## Rebooting a Device or Device Group

Using the WAAS Central Manager GUI, you can reboot a device or device group remotely.

To reboot an individual device, follow these steps:

- 
- Step 1** From the WAAS Central Manager GUI, choose **Devices > Devices**.
- Step 2** Click the **Edit** icon next to the name of the device that you want to reboot. The Device Home window appears.
- Step 3** In the taskbar, click the **Reload WAE** icon. You are prompted to confirm your decision.
- Step 4** Click **OK** to confirm that you want to reboot the device.
- 

To reboot a device from the CLI, use the **reload EXEC** command.

To reboot an entire device group, follow these steps:

- 
- Step 1** From the WAAS Central Manager GUI, choose **Devices > Device Groups**.
- Step 2** Click the **Edit** icon next to the name of the device group that you want to reboot. The Modifying Device Group window appears.
- Step 3** In the taskbar, click the **Reboot All Devices in Device Group** icon. You are prompted to confirm your decision.
- Step 4** Click **OK** to confirm that you want to reboot the device group.
- 

## Performing a Controlled Shutdown

A controlled shutdown refers to the process of properly shutting down a WAAS device without turning off the power on the device (the fans continue to run and the power LED remains on). With a controlled shutdown, all of the application activities and the operating system are properly stopped on the appliance, but the power remains on. Controlled shutdowns can help you minimize the downtime when the appliance is being serviced.



### Caution

If a controlled shutdown is not performed, the WAAS file system can be corrupted. It also takes longer to reboot the appliance if it was not properly shut down.

---

You can perform a controlled shutdown from the CLI by using the **shutdown EXEC** command. For more details, see the *Cisco Wide Area Application Services Command Reference*.

If you are running WAAS on a network module that is installed in a Cisco access router, perform a controlled shutdown from the router CLI by using the **service-module integrated-service-engine slot/unit shutdown EXEC** command. For more details, see the document *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.

