CHAPTER 15

Maintaining Your WAAS System

This chapter describes the tasks that 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 sections:

Upgrading the WAAS Software

Table 15-1 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 highest version. This is a change from WAAS version 4.0.x, where 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*.

If the WAAS Central Manager (version 4.1.1) sees any registered WAE devices that are at a higher version level, it raises a minor alarm to alert you. Additionally, the WAE devices are shown in red on the device listing page.

WAAS Central Manager version 4.1.1 can manage WAE devices that are running version 4.0.13 and later. Some WAAS Central Manager pages (with new features) will not be applicable to WAAS devices that are running a version lower than 4.1.1. If you modify the configuration on such pages, the configuration will be saved but it will have no effect on the device until the device is upgraded to version 4.1.1.

Note WAAS version 4.1.1 does not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.13. If you have any WAAS devices running version 4.0.11 or earlier, you must first upgrade them to version 4.0.13 (or a later 4.0.x version), before you install version 4.1.1. You should first upgrade any WAEs to version 4.0.13 (or a later 4.0.x version) and then upgrade any WAAS Central Managers to version 4.0.13 (or a later 4.0.x version). Then, you should begin the upgrade to version 4.1.1, starting with the WAAS Central Managers first.

Table 15-1 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 "Determining the Current Software Version" section on page 15-3.
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 "Obtaining the Latest Software Version from Cisco.com" section on page 15-3.
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 "Specifying the Location of the Software File in the WAAS Central Manager GUI" section on page 15-4.
4. Run the WAAS disk check tool.	Before you upgrade your WAE from version 4.0.3 or earlier, you must run a script (the WAAS disk check tool) that checks the file system for errors that can result from a RAID synchronization failure. For more information, see the "Using the WAAS Disk Check Tool" section on page 15-6.
5. Upgrade your WAAS Central Manager.	Upgrade the standby and primary WAAS Central Managers. For more information, see the "Upgrading the WAAS Central Manager" section on page 15-8.
6. Upgrade your WAAS devices using Device Groups.	After upgrading the WAAS Central Manager, upgrade all your WAAS devices that are members of a device group. For more information, see the "Upgrading Multiple Devices Using Device Groups" section on page 15-10.
7. Delete the software version file.	After completely upgrading your WAAS network, you can remove the software file if desired. For more information, see the "Deleting a Software File" section on page 15-10.

If you need to downgrade or roll back the WAAS software from version 4.1.1 to a lower version, first downgrade or roll back the WAE devices, then the standby Central Manager (if applicable), and finally the primary Central Manager. For more information about downgrading, see the *Release Note for Cisco Wide Area Application Services*.

Determining the Current Software Version

To view the current software version running on any particular device, choose **My WAN > Manage 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 Dashboard 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 navigation pane for any given device, choose **Admin > 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-4.1.1-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.

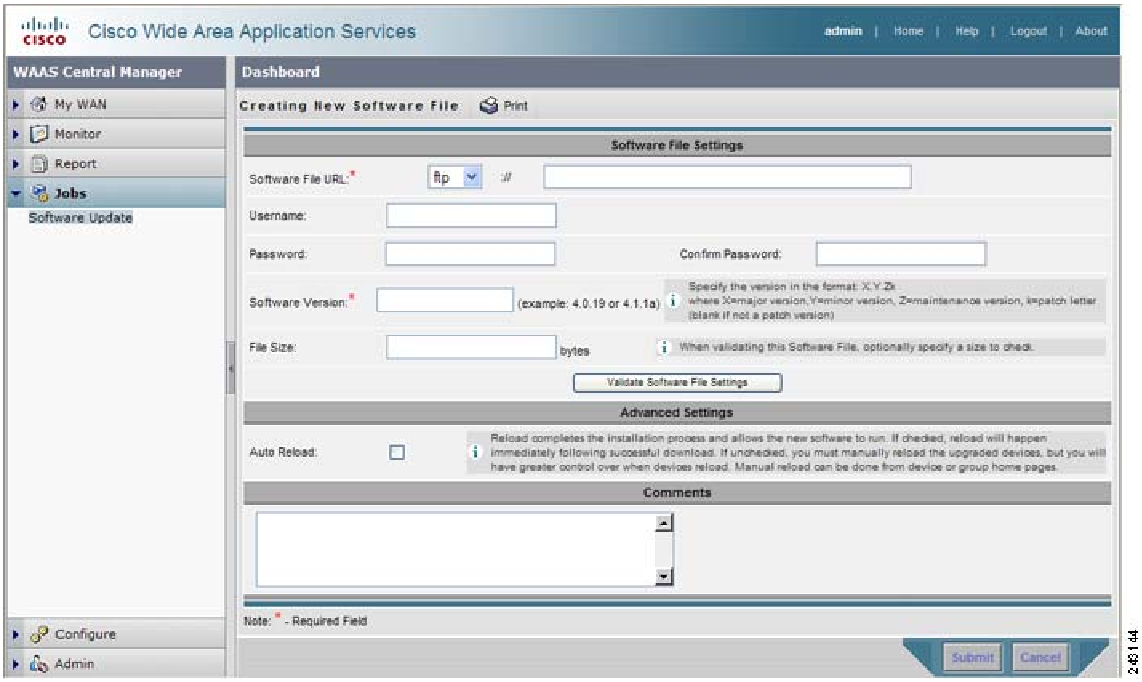
To configure the software file settings form, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **Jobs > Software Update**.

Step 2 Click the **Create New Software File** icon in the taskbar.

The Creating New Software File window appears. (See Figure 15-1.)

Figure 15-1 Creating New Software File Window



Specify the version in the format: X.Y.Zk where X=major version,Y=minor version, Z=maintenance version, k=patch letter (blank if not a patch version)

When validating this Software File, optionally specify a size to check.

Reload completes the installation process and allows the new software to run. If checked, reload will happen immediately following successful download. If unchecked, you must manually reload the upgraded devices, but you will have greater control over when devices reload. Manual reload can be done from device or group home pages.

Step 3 In the Software File URL field, specify the location of the new WAAS software file as follows:

a. Choose a protocol (**http** or **ftp**) from the drop-down list.

b. 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 this format: X.Y.Zk, where X = major version, Y = minor version, Z = maintenance version, and k= patch letter (not used if this is not a patch version).

Note If you are upgrading a version 4.0.x WAAS Central Manager to version 4.1.1, from a version 4.0.x WAAS Central Manager, enter 4.1.1.0.1 in the Software Version field. If you are upgrading to a maintenance release such as 4.1.1a, enter 4.1.1.a.1 in the Software Version field. For other maintenance releases, replace the “a” with the appropriate letter.

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.

Using the WAAS Disk Check Tool

Before you upgrade your WAE from version 4.0.3 or earlier, you must run a script (the WAAS disk check tool) that checks the file system for errors that can result from a RAID synchronization failure. (For more information about RAID synchronization, see the "Ensuring RAID Pairs Rebuild Successfully" section on page 15-7.) This script is not necessary when upgrading from WAAS version 4.0.5 or later, unless the system was running version 4.0.3 or earlier at some time in the past and the script was never run.

You can obtain the WAAS disk check tool from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/waas40

Note When you run the WAAS disk check tool, you will be logged out of the device. The device automatically reboots after it has completed checking the file system. Because this operation results in a reboot, we recommend that you perform this operation after normal business hours.

Copy the script to your WAE device by using the **copy ftp disk** command.

```
WAE# copy ftp disk <ftp-server> <remote_file_dir> disk_check.sh
```

Run the script from the CLI, as shown in the following example:

```
WAE# script execute disk_check.sh
This script will check if there is any file system issue on the attached disks
Activating the script will result in:
```

```
Stopping all services. This will log you out.
Perform file system check for few minutes.
and record the result in the following files:
/local1/disk_status.txt - result summary
/local1/disk_check_log.txt - detailed log
System reboot
If the system doesn't reboot in 10 minutes, please re-login and check the result files.
Continue?[yes/no] yes
Please disk_status.txt after reboot for result summary
umount: /state: device is busy
umount: /local/lPAM_unix[26162]: ### pam_unix: pam_sm_close_session (su) session closed
for user root
waitpid returns error: No child processes
No child alive.
```

After the device reboots and you log in, locate and open the following two files to view the file system status:

- disk_status.txt— Lists each file system and shows if it is “OK,” or if it contains an error that requires attention.
- disk_check_log.txt—Contains a detailed log for each file system checked.

If no repair is needed, then each file system will be listed as “OK,” as shown in the following example:

```
WAE# type disk_status.txt
Thu Feb 1 00:40:01 UTC 2007
device /dev/md1 (/swstore) is OK
device /dev/md0 (/sw) is OK
device /dev/md2 (/state) is OK
device /dev/md6 (/local/local1/spool) is OK
device /dev/md5 (/local/local1) is OK
device /dev/md4 (/disk00-04) is OK
```

If any file system contains errors, the disk_status.txt file instructs you to repair it.

Ensuring RAID Pairs Rebuild Successfully

You must ensure that all RAID pairs are done rebuilding before you reboot your WAE device. If you reboot while the device is rebuilding, you risk corrupting the file system.

RAID pairs will rebuild on the next reboot after you enable legacy WAFS core or edge services, use the **restore factory-default** command, replace or add a hard disk drive, delete disk partitions, or reinstall WAAS from the booted recovery CD-ROM.

To view the status of the drives and check if the RAID pairs are in “NORMAL OPERATION” or in “REBUILDING” status, use the **show disk details** EXEC command. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process can take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms indicating a problem:

- The device is offline in the Central Manager GUI.
- CMS can not be loaded.
- Error messages say that the file system is read-only.
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” and “ext3_readdir: bad entry in directory.”
- Other unusual behaviors related to disk operations or the inability to perform them.

If you encounter any of these symptoms, run the WAAS disk check tool to locate the problem.

Upgrading the WAAS Central Manager

When upgrading software in your WAAS network, begin with WAAS Central Manager before upgrading the WAE devices.

Note With WAAS version 4.0.x, you should upgrade the WAE devices before the WAAS Central Manager.

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 the primary WAAS Central Manager (version 4.1.1) sees that the standby WAAS Central Manager has a different version level, it shows the standby WAAS Central Manager in red on the device listing page.

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 (after the WAAS Central Manager).

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

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.

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

The Device Dashboard window appears.

Step 3 Verify that the device is not already running the version to which you plan to upgrade.

Step 4 Click the **Jobs > 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 15-4.

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 15-2 for a description of upgrade status messages.

Step 7 Close your browser and restart the browser session to the WAAS Central Manager, if you upgraded the primary 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.

Table 15-2 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 …)	The 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 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 navigation pane, choose **My WAN > Manage 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 navigation pane, choose **Jobs > Software Update**.

The Software Update for Device Group window appears.

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 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 15-4.

Step 5 Click **Submit**.

To view the progress of an upgrade, go to the Devices window (**My WAN > Manage 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 15-2 for a description of the 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 navigation pane, choose **Jobs > Software Update**.

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 15-11
- Backing Up and Restoring a WAE Device, page 15-13
- Using the Cisco WAAS Software Recovery CD-ROM, page 15-13
- Recovering the System Software, page 15-17
- Recovering a Lost Administrator Password, page 15-19
- Recovering from Missing Disk-Based Software, page 15-20
- Recovering WAAS Device Registration Information, page 15-21

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 back up print drivers. When you perform a Central Manager database backup, you must reinstall your print drivers if you are using WAAS print services.

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

You should 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 apply only 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 15-11.

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 10-7.
- CLI—You can use the following commands to back up and restore a device's database:
  - **wafs backup-config**—Saves the entire legacy WAFS system configuration to a file, including the 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.

The 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 WAAS software to work properly.

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

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

  An installation that contains 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.

These options 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 performed automatically 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 installed automatically.

  This option is performed automatically 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. You need to use this option only if there has been a change in the hardware components, such as replacing the motherboard, or if you moved a flash memory card between systems.

  This option is performed automatically 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 WAAS software.

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

This option performs the following steps:

a. 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.

b. Erases data from all drives.

c. Remanufactures the default Cisco file system layout on the disk.

d. Installs the flash memory component from the .bin image.

e. Installs the disk component from the .bin image.

- Option 8: Recreate RAID device—This option appears only for WAE-7341, WAE-7371, and WAE-674 devices and recreates the RAID array.
- Option 9: Exit and Reboot—This option reboots the device. Remove the CD-ROM before rebooting in order to boot from flash memory. (For all WAE devices except WAE-7341, WAE-7371, and WAE-674 devices, this option is Option 8.)

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 4.1.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. Recreate RAID device
  9. Exit (and reboot)
Choice [0]:
```

Option 8 appears only for WAE-7341, WAE-7371, and WAE-674 devices. For other devices, option 8 is Exit (and reboot).

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 (Optional) If you are working with a WAE-7341, WAE-7371, or WAE-674 device, choose option 8 to recreate the RAID array.

Step 8 Choose option 7 to wipe the disks and install the binary image.

This step prepares the disks by erasing them. The WAAS 4.1.x image is installed.

Step 9 Remove the CD-ROM from the drive.

Step 10 Choose the option (8 or 9, depending on your WAE model) to reboot the WAE.

After the WAE reboots, it is running the WAAS 4.1.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-4.1.1-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-4.1.1-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-4.1.1-k9.bin
```

Step 6 Reload the module:

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

After the module reboots, it is running the WAAS 4.1.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-4.1.1-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-4.1.1-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) 1999-2008 by Cisco Systems, Inc.
Wide Area Application Services Release 4.1.1
Version: ce507-5.2.0

Compiled 02:34:38 May 8 2008 by (cisco)
Compile Time Options: PP SS



System was restarted on Thu June 22 16:03:51 2008.
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 You cannot 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**

```
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 cleartext or encrypted.

Note Do not set the user ID (uid).

Step 6 Save the configuration change:

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

Step 7 (Optional) Reboot your device:

```
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 the WAAS software, the bootflags are reset to 0x0 on every reboot.

Recovering from Missing Disk-Based Software

This section describes how 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 automaticaly 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 navigation pane, go to **My WAN > Manage Devices**.
- **b.** Click the **Edit** icon next to the device that you want to deactivate.
- **c.** From the navigation pane, choose *Device Name* **> Activation**. The Device Activation window appears.
- **d.** Uncheck the **Activate** check box, and 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 the 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 15-21.

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 GUI, choose **My WAN > Manage Devices**.
- **b.** Click the **Edit** icon next to the device that you want to deactivate. The Device Dashboard window appears.
- **c.** In the navigation pane, choose *Device Name* **> Activation**.
- **d.** Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.
- **e.** Check the **Replaceable** check box, and click **Submit**.

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

Step 2 Configure a system device recovery key as follows:

- **a.** From the WAAS Central Manager GUI navigation pane, choose **Configure > System Properties**.
- **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:

a. From the WAAS GUI, choose **My WAN > Manage Devices**.

b. Click the **Edit** icon next to the WAAS device that you want to activate. The Device Dashboard window appears.

c. In the navigation pane, choose *Device Name* **> Activation**. The WAAS device status should be Online.

d. Check the **Activate** check box, and click **Submit**.

Performing Disk Maintenance for RAID-1 Systems

WAAS supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. When a disk fails, WAAS automatically detects the disk failure, marks the disk as bad, and removes the disk from the RAID-1 volume. To schedule disk maintenance, you must manually shut down the disk.

You must wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog ERROR message is logged.

Note If the removal event (such as, a disk failure or software shutdown) occurs while the RAID array is in the rebuild process, the RAID removal process may take up to 1 minute to complete. The duration of this process depends on the size of the disk.

If the WAAS software removes a failed disk during the RAID rebuild process, a RAID rebuild failure alarm is generated. If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

When you install a replacement disk, the WAAS software detects the replacement disk and performs compatibility checks on the disk, initializes the disk by creating partitions, and adds the disk to the software RAID to start the RAID rebuild process.

If the newly inserted disk has the same disk ID as a disk that was previously marked bad in the same physical slot, then the disk will not be mounted, and the post-replacement checks, initialization, and RAID rebuilding will not occur.

A newly installed disk must be of the same type as the old disk and it must meet the following compatibility requirements:

- If the replacement disk is for disk00, disk02, or disk04 of a RAID pair, the replacement disk must be the same size as the running disk in the array.
- If the replacement disk is for disk01, disk03, or disk05 of a RAID pair, then the replacement disk must have the same or greater RAID capacity as the running disk in the array.

Compatibility checks, which are part of the hot-swap process, check for capacity compatibility. Incompatibility generates an alarm and aborts the hot-swap process.

Table 15-3 shows the drive-type compatibility for the WAE-612. All drives must be the same type.

Table 15-3 WAE-612 Drive-Type Compatibility Matrix

Drive Types	SAS[1]	SATA2[2]
SAS	Ok	No
SATA2	No	Ok

[1] Serial Attached SCSI

[2] Serial Advanced Technology Attachment 2

To perform disk maintenance, follow these steps:

Step 1 Manually shut down the disk.

a. Enter the **disk disk-name** *diskxx* **shutdown** command in global configuration mode.

b. Wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, WAAS generates a disk failure alarm and trap. In addition, a syslog ERROR message is logged.

Note We recommend that you disable the **disk error-handling reload** option, if enabled, because it is not necessary to power down the system to remove a disk.

Step 2 Insert a replacement disk into the slot in the WAE. The replacement disk must have a disk ID number that is different from the disk that it is replacing.

Step 3 Reenable the disk by entering the **no disk disk-name** *diskxx* **shutdown** global configuration command.

Replacing Disks in RAID-5 Systems

To remove and replace a physical disk drive in a system that uses a RAID-5 logical drive, follow these steps:

Step 1 Enter the **disk disk-name** *diskxx* **replace** command in EXEC mode at the WAAS CLI on the WAE.

Step 2 Verify that the disk drive *diskxx* is in the Defunct state by entering the **show disks details** command in EXEC mode. The RAID logical drive is in the Critical state at this point.

Step 3 Move the handle on the drive to the open position (perpendicular to the drive).

Step 4 Pull the hot-swap drive assembly from the bay.

Step 5 Wait for one minute and then insert the new drive into the same slot by aligning the replacement drive assembly with guide rails in the bay and sliding the drive assembly into the bay until it stops. Make sure that the drive is properly seated in the bay.

Step 6 Close the drive handle.

Step 7 Check the hard disk drive status LED to verify that the hard disk drive is operating correctly. If the amber hard disk drive status LED for a drive is lit continuously, that drive is faulty and must be replaced. If the green hard disk drive activity LED is flashing, the drive is being accessed.

Step 8 Wait 1 minute and then verify that the replaced disk drive is in the Rebuilding state by using the **show disks details** command in EXEC mode.

Note The ServeRAID controller automatically starts the rebuild operation when it detects the removal and reinsertion of a drive that is part of the logical RAID drive.

Step 9 Wait until the rebuild operation is complete. You can check if the rebuild operation is complete by using the **show disks details** command in EXEC mode. The physical drive state will be Online and the RAID logical drive state will be Okay after the rebuild operation is completed.

A 300-GB SAS drive may take up to 5 hours to finish rebuilding.

If you have multiple disk failures and your RAID-5 logical status is Offline, you must recreate the RAID-5 array by following these steps:

Step 1 Enter the **disk logical shutdown** command in global configuration mode to disable the RAID-5 array.

Step 2 Enter the **write** command in EXEC mode to save the running configuration to NVRAM.

Step 3 Enter the **reload** command in EXEC mode to reload the system.

Step 4 Enter the **show disks details** command in EXEC mode to check the system configuration after the system is rebooted. At this point, the disks are not mounted and the logical RAID drive should be in the Shutdown state.

Step 5 Enter the **disk recreate-raid** command in EXEC mode to recreate the RAID-5 array.

Step 6 After successful execution of the previous command, enter the **no disk logical shutdown** command in global configuration mode to disable the logical disk shutdown configuration.

Step 7 Enter the **write** command in EXEC mode to save the configuration to NVRAM.

Step 8 Enter the **reload** command in EXEC mode to reload the system.

Step 9 Enter the **show disks details** command in EXEC mode to check the system configuration after the system is rebooted. At this point, the disks should be mounted and the logical RAID drive should not be in the Shutdown state.

Step 10 Wait until the rebuild operation is complete. You can check if the rebuild operation is complete by using the **show disks details** command in EXEC mode. The physical drive state will be Online and the RAID logical drive state will be Okay after the rebuild operation is completed.

It takes several hours to finish rebuilding the RAID-5 array.

Switching a WAAS Central Manager from Standby to Primary

The 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 if you are using WAAS print services. 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 Ensure 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 Ensure 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:

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

b. Switch the original standby to primary mode:

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

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

Enabling Disk Encryption

Disk encryption addresses the need to securely protect sensitive information that flows through deployed WAAS systems and that is stored in WAAS persistent storage. The disk encryption feature includes two aspects: the actual data encryption on the WAE disk and the encryption key storage and management.

When you enable disk encryption, all data in WAAS persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored on the Central Manager, and key management is handled by the Central Manager. When you reboot the WAE after configuring disk encryption, the WAE retrieves the key from the Central Manager automatically, allowing normal access to the data that is stored in WAAS persistent storage.

Note If a WAE is unable to reach the WAAS Central Manager during a reboot, it will do everything except mount the encrypted partitions. In this state, all traffic will be handled as pass-through. Once communication with the WAAS Central Manager is restored (and the encryption key is obtained), the encrypted partitions are mounted. There is no loss of cache content.

Disk encryption requirements are as follows:

- You must have a Central Manager configured for use in your network.
- Your WAE devices must be registered with the Central Manager.
- Your WAE devices must be online (have an active connection) with the Central Manager. This requirement applies only if you are enabling disk encryption.
- You must reboot your WAE for the disk encryption configuration to take effect.

  After you reboot your WAE, the encryption partitions are created using the new key, and any previously existing data is removed from the partition.

Any change to the disk encryption configuration, whether to enable or disable encryption, causes the disk to clear its cache. This feature protects sensitive customer data from being decrypted and accessed should the WAE ever be stolen.

If you enable disk encryption and then downgrade to a software version that does not support this feature, you will not be able to use the data partitions. In such cases, you must delete the disk partitions after you downgrade.

To enable and disable disk encryption from the Central Manager GUI, choose **My WAN > Manage Devices**, choose a device, then choose **Configure > Storage > Disk Encryption**. To enable disk encryption, check the **Enable** check box and click **Submit**. This box is unchecked by default. To disable disk encryption, uncheck the **Enable** check box and click **Submit**.

To enable and disable disk encryption from the WAE CLI, use the **disk encrypt** global configuration command.

When you enable or disable disk encryption, the file system is reinitialized during the first subsequent reboot. Reinitialization may take from ten minutes to several hours, depending on the size of the disk partitions. During this time, the WAE will be accessible, but it will not be providing any services.

If you change the Central Manager IP address, or if you relocate the Central Manager, or replace one Central Manager with another Central Manager that has not copied over all of the information from the original Central Manager, and you reload the WAE when disk encryption is enabled, the WAE file system will not be able to complete the reinitialization process or obtain the encryption key from the Central Manager.

If the WAE fails to obtain the encryption key, disable disk encryption by using the **no disk encrypt enable** global configuration command from the CLI, and reload the WAE. Ensure connectivity to the Central Manager before you enable disk encryption and reload the WAE. This process will clear the disk cache.

Note When a standby Central Manager has been in service for at least 2 times the datafeed poll rate time interval (approximately 10 minutes) and has received management updates from the primary Central Manager, the updates will include the latest version of the encryption key. Failover to the standby in this situation occurs transparently to the WAE. The datefeed poll rate defines the interval for the WAE to poll the Central Manager for configuration changes. This interval is 300 seconds by default.

To view the encryption status details, use the **show disks details** EXEC command. While the file system is initializing, **show disks details** displays the following message: "`System initialization is not finished, please wait...`" You may also view the disk encryption status, whether it is enabled or disabled, in the Central Manager GUI, Device Dashboard window.

Configuring a Disk Error-Handling Method

Note Configuring and enabling disk error handling, in particular the **reload** option, is no longer necessary for devices that support disk hot-swap. In WAAS 4.0.13 and later, the software automatically removes from service any disk with a critical error.

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 navigation pane, choose **My WAN > Manage Devices** (or **Manage 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 In the navigation pane, choose **Configure > Storage > Disk Error Handling**.

The Disk Error Handling Settings window appears.

Step 4 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 5 Click **Submit** to save the settings.

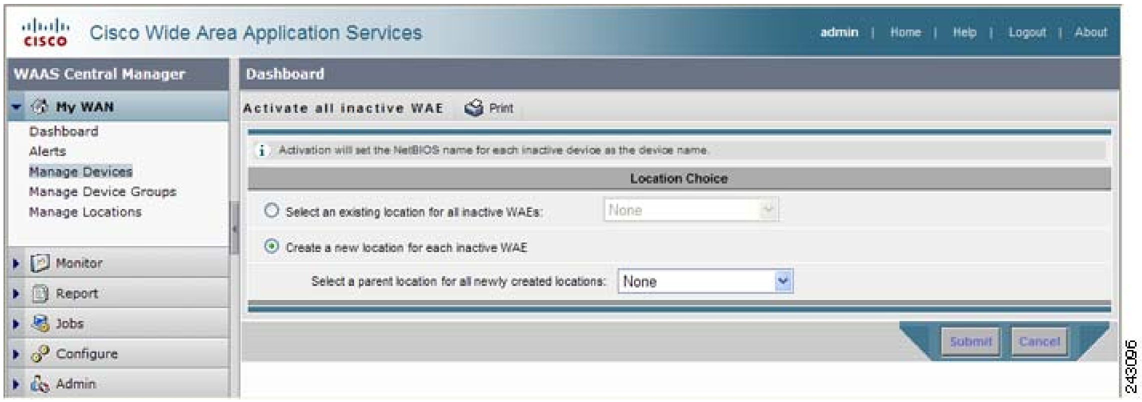
Activating All Inactive WAAS Devices

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

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage 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 15-2.)

Figure 15-2 Activating Inactive Devices



Activation will set the NetBIOS name for each inactive device as the device name.

Location Choice

○ Select an existing location for all inactive WAEs: None

● Create a new location for each inactive WAE

Select a parent location for all newly created locations: None

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 GUI, choose **My WAN > Manage Devices**.

Step 2 Click the **Edit** icon next to the name of the device that you want to reboot. The Device Dashboard 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.

If you reboot a WAAS Central Manager that has the secure store enabled, you must reopen the secure store after the reboot by using the **cms secure-store open** EXEC command.

To reboot an entire device group, follow these steps:

Step 1 From the WAAS GUI, choose **My WAN > Manage 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*.