Maintaining Your WAAS System

This chapter describes the tasks that you should perform to maintain your WAAS system.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and WAVE appliances, Cisco Service-Ready Engine service modules (SRE-SM) running Cisco WAAS, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

Upgrading the WAAS Software

Table 14-1 outlines the steps that you must complete to upgrade your WAAS software to the latest version.

We recommend that all the devices in your WAAS network run 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 latest version. For details on version interoperability limitations, see the *Release Note for Cisco Wide Area Application Services*.

If the Central Manager sees any registered WAE devices that are at a higher version level than the current one, 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 5.4.1 can manage WAE devices running Version 4.3.1 and later. Some WAAS Central Manager windows (with new features) are not applicable to WAAS devices that are running a version lower than 5.4.1. If you modify the configuration in such windows, the configuration is saved, but it has no effect on the device until the device is upgraded to Version 5.4.1.

Note WAAS Version 5.4 is not supported running in a mixed-version WAAS network, where any WAAS device is running a software version lower than 4.3.1. If you have WAAS devices running versions earlier than 4.3.1, you must first upgrade them to Version 4.3.1 (or a later version) before you install version 5.2 on the Central Manager. Do not upgrade any device to a version later than the existing Central Manager version. After all the devices are upgraded to Version 4.3.1 or a later, you can begin the upgrade to Version 5.4.1 on the WAAS Central Manager. Directly upgrading a device from Version 4.0, 4.1 or 4.2 to 5.4.1 is not supported.

Note When a SM-SRE device registered to a Central Manager (both running the same software version) is downgraded to a lower version, the SM-SRE device goes offline. You need to de-register the device from the Central Manager and reload it twice for the configuration to take effect. Next you need to register the device to the Central Manager for it to work properly.

Upgrading is supported only from certain older releases to a particular release. If you have a WAAS device that is running a release from which upgrading to the desired release is not supported, first upgrade the device to an intermediate supported release and then to the final desired release. For details on what versions are supported for upgrades, see the *Release Note for Cisco Wide Area Application Services* for the software version to which you want to upgrade.

Note Before starting the upgrade, disable WCCP on all WAEs in an AppNav cluster. After upgrade is complete, confirm the following before you re-enable WCCP.

- The WAEs are up and running.
- The AppNav cluster is re-converged properly.
- All disks are ready (not initializing).
- No alarms on the device.
- The **show accelerator** command shows all enabled Application Optimizers are healthy.

After you have confirmed that each of these is complete, you can re-enable WCCP.

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 Determining the Current Software Version.

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 Obtaining the Latest Software Version from Cisco.com.
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 Specifying the Location of the Software File in the WAAS Central Manager GUI.
4. Upgrade your WAAS Central Manager.	Upgrade the standby and primary WAAS Central Managers. For more information, see Upgrading the WAAS Central Manager.
5. 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 Upgrading Multiple Devices Using Device Groups.
6. Delete the software version file.	After completely upgrading your WAAS network, you can remove the software file if desired. For more information, see Deleting a Software File.

Installing a software version on a SM-SRE device from a router using IPv6 address is not supported.

To downgrade or roll back the WAAS software to a lower version, first downgrade or roll back the WAE devices' version, 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 a particular device, choose **Devices > All Devices**. The All Devices window displays the software version for each listed device.

You can also click **Devices >** *device-name* or 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 is 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 device context, choose **Monitor > CLI Commands > Show Commands**. Choose **version** and click **Submit**. A secondary window is displayed with 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 web browser and access the cisco.com website:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Navigate to the **Application Networking Services** > **Wide Area Application Services** > **Cisco Wide Area Application Services (WAAS) Software** download area.

Step 3 Choose the WAAS software version that you want and download the appropriate software image.

Step 4 Register the location of the software file in the WAAS Central Manager GUI, as described in Specifying the Location of the Software File in the WAAS Central Manager GUI.

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.

There are two types of WAAS software files:

- Universal—Includes Central Manager, Application Accelerator, and AppNav Controller functionality. You can use this type of software file to upgrade a device operating in any mode.
- Accelerator only—Includes Application Accelerator and AppNav Controller functionality only. You can use this type of software file to upgrade only an Application Accelerator or AppNav Controller device. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must install the Universal software file, reload the device, change the device mode to central-manager, and then reload the device again. Additionally, kdump analysis functionality is not included in the Accelerator only image.

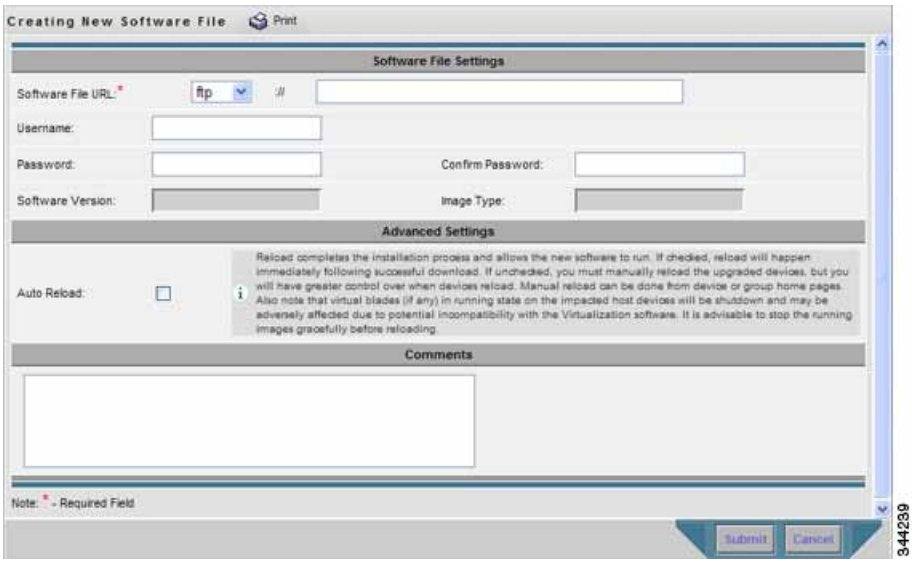
To configure the software file settings form, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin** > **Version Management** > **Software Update**.

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:

a. Choose a protocol (**http** or **ftp**) from the **Software File URL** 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-xxxx-K9*.bin

http://2012:3:3:3::8/waas/*WAAS-xxxx-K9*.bin

Here, WAAS-*xxxx*-K9.bin is the name of the software upgrade file. (The filename typically includes the version number.)

Be sure that the URL identifies the correct type of software image for the devices you want to upgrade, either Universal or Accelerator only.

If the Central Manager has been configured with an IPV6 address, it can be accessed using https://[CM ipv6 address]:8443/

Software update configuration with IPv6 address will be filtered in the device /device group level usage pages for unsupported device models / versions.

Step 4 (Optional) 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.

The **Software Version** and **Image Type** fields cannot be edited. They are filled in automatically after you submit the settings and the image is validated.

Step 5 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 check box, you should manually reload a device after you upgrade the software on it to complete the upgrade process.

Step 6 (Optional) Enter comments in the **Comments** field.

Step 7 Click **Submit**.

The software image file is validated and the Software Version and Image Type fields are filled in with the appropriate information extracted from the image file.

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.

Note When you are viewing the list of registered software files, if the Image Type column shows Unknown for a software file, it indicates that the software file was added under a WAAS version previous to 4.2.1. These Unknown software files must be resubmitted if you want to use them. Click the **Edit** icon next to the file to open the Modifying Software File window, and then click the **Submit** button to resubmit the file.

Upgrading the WAAS Central Manager

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

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 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, and 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 menu, choose **Devices** > *device-name*.

The Device Dashboard window appears.

Step 2 Verify that the device is not already running the version to which you plan to upgrade.

Step 3 Click the **Update** link.

The Software Update window appears.

Step 4 Choose the software file URL from the Software Files list by clicking the radio button next to the corresponding filename.

The list displays only software files with an image type of Universal, because you are upgrading a Central Manager device. If no such images are available, you must create a software file, as described in Specifying the Location of the Software File in the WAAS Central Manager GUI.

Step 5 Click **Submit**, and then click **OK** to confirm your decision.

The Devices Listing window is displayed again. 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.

Step 6 Clear your browser cache, close the browser, and restart the browser session to the WAAS Central Manager.

The WAAS Central Manager may reboot at the conclusion of the upgrade procedure (if **Auto Reload** is in the Creating New Software File window), causing you to temporarily lose contact with the device and the GUI.

Table 14-2 Upgrade Status Messages

Upgrade Status Message	Condition
Pending	The request is yet to be sent from the WAAS Central Manager to the device, or receipt of the request is 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 a 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 is successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log. If you are upgrading several devices at once, the download may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.
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.

Table 14-2 Upgrade Status Messages (continued)

Upgrade Status Message	Condition
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. If you are upgrading several devices at once, the upgrade may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.

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 menu, choose **Device Groups** > *device-group-name*.

Step 2 Choose **Admin** > **Versioning** > **Software Update**.

The Software Update for Device Group window appears.

Step 3 Choose the software file URL from the Software File URL list by clicking the radio button next to the filename. If no images are available, create a software file, as described in Specifying the Location of the Software File in the WAAS Central Manager GUI.

If you are updating many devices and you want to use a smaller size software file to save network bandwidth, specify a software file with an image type of Accelerator only, which is smaller than a Universal image. If you later want to change an Accelerator-only device to a Central Manager, you must install the Universal software file, reload the device, change the device mode to central-manager, and then reload the device again.

Step 4 Click **Submit**.

To view the progress of an upgrade, go to the All Devices window (**Devices** > **All 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.

Upgrading Central Manager to New Hardware and Converting an Existing Central Manager to a WAE

If you want to add a new piece of hardware as a primary Central Manager and want to use the existing Central Manager as a WAE, it is important to first add it to the system and then configure it.

Note Performing a database backup of the former Central Manager and restoring it on the new device prevents it from being used as a WAE later.

To upgrade to a new Central Manager and convert an existing Central Manager to a WAE, follow these steps:

Step 1 Add a hardware device as the new Central Manager and configure it as a standby Central Manager. There might be multiple standby Central Managers in the system. For more information, see Configuring the Central Manager Role.

Step 2 Enable the new hardware device to be the primary Central Manager after it is available online and has finished synchronizing with other systems. For more information, see Converting a Standby Central Manager to a Primary Central Manager

Step 3 Disable CMS service and execute the **cms deregister** command at the former Central Manager CLI interface to remove it from the CM database. If there is no connectivity between the devices anymore, use the **cms deregister force** command and manually delete the former Central Manager in the new Central Manager GUI.

```
wae# cms deregister force
Deregistering WAE device from Central Manager will result in loss of data on encrypted
file systems, imported certificate/private keys for SSL service and wafs preposition
credentials. If secure store is initialized and open, clear secure store and wait for one
datafeed poll rate to retain wafs preposition credentails.
Do you really want to continue (yes|no) [no]?yes Disabling management service.
management services stopped
Sending de-registration request to CM
Failed to contact CM(Unmarshaled: 9001). Please check connectivity with CM device and
status of management service on CM.
Device de-regsitration failed, removing device registration information.
Please delete the device record on the Central Manager.
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.Deregistration complete.
Save current cli configuration using 'copy running-config startup-config' command because
CMS service has been disabled.
#
```

Step 4 Rename the former Central Manager, change the IP address, change its mode using the **device mode** command, and reload using the **reload** command:

```
wae# configure
wae(config)# device mode application-accelerator
The new configuration will take effect after reload.
wae# reload
```

Step 5 Rename the new primary Central Manager and change its IP address to fully replace the former one. Otherwise, you will need to update the configuration of your devices to point to the new address of the Central Manager. Contact a Cisco TAC member for scripts.

```
wae(config)# hostname old primary central-manager name
wae(config-if)# ip address ipaddress netmask.
```

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 that you may have to downgrade your system for any reason.

To delete a software file, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Version Management > 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**.

The selected software file is 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

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 that 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, specify the location, password, and user ID of the remote server that you want to store the backup file in. If you want to back up only the configuration information, use the **cms database backup config** EXEC command.

Note If you have already performed a backup when the secure store was in user-passphrase mode and you restored it to a system where the secure store is in auto-passphrase mode, you must enter the user passphrase to proceed with the restore. After the restore, the system is in user-passphrase mode. If you already performed a backup when the secure store was in auto-passphrase mode and you restored it to a system where the secure store is in user-passphrase mode, you do not have to enter a password. After the restore, the system is in auto-passphrase mode.

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

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

```
CM# cms database backup
Creating database backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1.dump
Backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1 is ready.
Please use `copy' commands to move the backup file to a remote host.
```

Note The backup file is automatically given a name in the format cms-db-*date-timestamp_version*.dump, for example, cms-db-7-22-2010-17-36_4.3.1.0.1.dump. Note that the timestamp is in a 24-hour format (HH:MM) that does not show seconds. It is stored in /local1/backup.

Step 2 Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from a local disk to a remote FTP server.

```
CM# cd /local1/backup
CM# copy disk ftp 10.86.32.82 /incoming cms-db-7-22-2008-17-36_4.1.3.0.1.dump
cms-db-7-22-2008-17-36_4.1.3.0.1.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 cms-db-7-22-2008-17-36_4.1.3.0.1.dump
Opening BINARY mode data connection for cms-db-7-22-2008-17-36_4.1.3.0.1.dump.
Transfer complete.
Sent 18155 bytes
```

Step 3 Restore the CMS database as follows:

a. Disable the CMS service:

```
CM# configure
CM(config)# no cms enable
CM(config)# exit
```

Note Stopping the CMS service disables the WAAS Central Manager GUI. All the users who are currently logged in to this GUI are automatically logged out after the CMS service is disabled.

b. Delete the existing CMS database:

```
CM# cms database delete
```

c. Initialize the CMS database:

```
CM# cms database create
```

d. Restore the CMS database contents from the backup file:

```
CM# cms database restore backup/cms-db-7-22-2008-17-36_4.1.3.0.1.dump
```

Note After the restore, any WAEs that were registered with the Central Manager during the time since the backup was created will be disconnected from the Central Manager because there is no information about them in the backup file. To bring these WAEs online, you must deregister and reregister them with the Central Manager. On each WAE that was disconnected, use the following commands:

```
WAE# cms deregister force
WAE# configure
WAE(config)# cms enable
```

e. Enable the CMS service on the Central Manager:

```
CM# configure
CM(config)# cms enable
```

Note If you want to upgrade the Central Manager to a newer model, backing up the former Central Manager's database and restoring it on the new device prevents it from being used as a WAE later. For more information, see the "Upgrading Central Manager to New Hardware and Converting an Existing Central Manager to a WAE" section on page 14-8.

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 occurs.

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 Backing Up and Restoring the WAAS Central Manager Database.

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

- CLI—Use the **copy running-config** command to back up and restore a device's configuration. This command saves the currently running 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 the 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 Guide*.

Reinstalling the System Software

This section contains instructions for using the software recovery files to reinstall your system software if for some reason the software that is installed has failed. A software recovery CD-ROM ships with some WAE and WAVE hardware devices. Some WAVE devices use a USB flash drive for recovery.

Caution If you upgraded your software after you received your software recovery CD-ROM or image files, using the recovery software images may downgrade your system. Ensure that you are using the desired software recovery version.

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 (the Universal version of the WAAS software)
- 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.

Note The system image that is used depends on your device. For all WAVE devices (64-bit platforms), use the 64-bit system image (with "x86_64" in its name). For all other devices, use the 32-bit system image named without this designator.

A Network Processing Engine (NPE) image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted, is provided.

If you have a WAVE appliance that requires a USB flash drive for software recovery, your USB flash drive must contain both of the needed software images in the form of an ISO archive file that you copy to the flash drive. (See Preparing the USB Flash Drive).

These options are available from the software recovery installer menu:

- Option 1: Configure Network—If the .bin image you need to install is located on the network instead of the CD-ROM or USB flash drive (which may be the case when an older CD-ROM or USB image 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. 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 USB/CD-ROM —These options allow installation of only the flash memory .sysimg and do not modify disk contents. They can be used when a new chassis has been provided and populated with a 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: Re-create RAID device—This option applies only to WAVE-7541, WAVE-7571, and WAVE-8541 devices and re-creates the RAID array.

- Option 8: Wipe Out Disks and Install .bin Image—This option provides the preferred procedure for installing the WAAS software.

Caution Option 8 erases the content from the 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. Re-manufactures 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.

Note When Option 8 is used and the system reboots and begins optimizing traffic, the **show disks details** command may show that 98% or more of the /dre1 partition has been used due to the preallocation of DRE cache space. Use the **show statistics dre** command to display the actual DRE cache usage.

- Option 9: Exit (reboot)—This option ejects the CD-ROM (if applicable) and reboots the device. If you are using a USB flash drive for software installation, remove it from the device before rebooting.

The following sections describe how to reinstall the WAAS system software:

- Preparing the USB Flash Drive—Read this section if you have a WAVE appliance that requires a USB flash drive instead of a CD to install the system software.
- Reinstalling the System Software—Describes how to reinstall the system software from a CD or USB flash drive.
- Ensuring that RAID Pairs Rebuild Successfully—Describes how to ensure that RAID disks rebuild successfully.

Preparing the USB Flash Drive

If you have a WAVE appliance that requires a USB flash drive for software recovery, you must prepare the USB flash drive with the appropriate files before you can start the software recovery process. You will need the following:

- Windows PC (Windows XP or 7) or Mac computer
- USB flash drive that is 1 GB or larger in size
- The following software recovery files:
  - WAAS Rescue CD ISO image file, which is available in the WAAS Software Download area of Cisco.com. The filename is similar to waas-rescue-cdrom-*x.x.x.x*-k9.iso, where the *x*'s denote the software version number. Alternatively, the ISO image file is available on the WAAS release DVD, or you can make an ISO image file from a WAAS recovery CD.
  - The syslinux.cfg file, which is also available in the WAAS Software Download area of Cisco.com and on the WAAS release DVD.
  - Unetbootin utility for Windows or MAC, which is available from the Unetbootin Sourceforge website.

To prepare the USB flash drive on a Windows or MAC computer, follow these steps:

Step 1 Transfer the software recovery files on to the computer, noting the directory in which they are stored.

Step 2 Insert the USB flash drive into a USB port on the computer.

Step 3 Open My Computer (Windows) or Disk Utility (MAC).

Step 4 Format the USB flash drive:

- For Windows, right click the **Removable Disk** (drive letter will vary with system) and select **Format**.
  - In the formatting tool, from the **File System** drop-down list, select FAT32.
  - In the **Format Options** sections, check the **Quick Format** check box, and then click **Start**.
  - Click OK on the warning message.
  - Close the formatting tool after the formatting is complete.
- For MAC, select the USB drive on the left side of window, and use the **Erase** tab to format for use with MS-DOS (FAT).

Step 5 Launch the Unetbootin utility.

Step 6 Select the Diskimage option and click the corresponding **browse** button (...) to select the waas-rescue-cdrom-*x.x.x.x*-k9.iso image file.

Step 7 Ensure that USB Drive is selected in the **Type** drop-down list and that the correct drive letter is selected for **Drive**.

Step 8 Click **OK** to install the bootable image in the USB flash drive. When the installation has completed, click **Exit**.

Step 9 Drag a copy of the syslinux.cfg file into the USB flash drive and click Yes to confirm the replacement. This file replaces the existing file on the USB flash drive with the one customized for your WAAS system.

Step 10 Remove the USB flash drive from the computer.

To continue reinstalling the system software from the prepared USB flash drive, follow the instructions in Reinstalling the System Software.

Reinstalling the System Software

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

Step 1 Connect a serial console to the WAAS appliance and use the console for the following steps.

Step 2 Insert the software recovery CD-ROM in the CD drive of the WAE device or, if the device uses a USB flash drive for recovery, insert a bootable USB flash drive with the software recovery files into the USB port of the device (see Preparing the USB Flash Drive). WAVE-294/594/694/7541/7571/8541 devices do not have CD drives; they use a USB flash drive for software recovery.

Step 3 Reboot the WAE. During the boot process, the boot loader pauses for 30 seconds and you must choose the VGA console if you are using vWAAS. The prompt is displayed as follows:

```
Type "serial" for WAE/WAVE appliance.
Type "vga" for vWAAS.
boot:
```

Enter the **vga** command at the prompt to continue the boot process for the VGA console on vWAAS. After 30 seconds with no input, the boot process continues with the standard serial console for WAAS appliances.

After the WAE boots, you will see the following:

```
Installer Main Menu:
  1. Configure Network
  2. Manufacture flash
  3. Install flash cookie
  4. Install flash image from network
  5. Install flash image from usb/cdrom
  6. Install flash image from disk
  7. Recreate RAID device (WAE-7541/7571/8541 only)
  8. Wipe out disks and install .bin image
  9. Exit (reboot)
Choice [0]:
```

Note The option numbers in the installer main menu may vary, depending on the WAAS software release being installed.

Step 4 Choose Option 2, “Manufacture flash,” 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, “Install flash cookie,” to install the flash cookie that you prepared in the previous step.

Step 6 Choose Option 5, “Install flash image from usb/cdrom,” to install the flash image from a CD-ROM or USB flash drive.

Step 7 (Optional) If you are working with a WAVE-7541, WAVE-7571, or WAVE-8541 device, choose option 7 to recreate the RAID array.

Step 8 Choose Option 8, “Wipe out disks and install .bin image,” to wipe the disks and install the binary image.

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

Step 9 If you are using a USB flash drive to install the software, remove it from the device.

Step 10 Choose Option 9, “Exit (reboot),” to reboot the WAE.

After the WAE reboots, it runs the newly installed WAAS 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 in the module:

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

Step 3 While the module is loading, 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 is displayed. The following example shows how to interact with the Rescue Image dialog box (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-5.1.1.10-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-5.1.1.10-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-5.1.1.10-k9.bin
```

Step 6 Reload the module:

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

After the module reboots, it runs the newly installed WAAS software.

Ensuring that RAID Pairs Rebuild Successfully

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

RAID pairs will rebuild on the next reboot after you 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 or USB flash drive.

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 cannot be loaded.
- Error message stating that the file system is read-only is displayed.

The syslog contains errors such as:

```
—Aborting journal on device md2
—Journal commit I/O error
—Journal has aborted
—ext3_readdir: bad entry in directory
```

- Other unusual behaviors related to disk operations or the inability to perform them are visible.

If you encounter any of these symptoms, reboot the WAE device and wait until the RAID rebuild finishes normally.

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 help you download a system image to the main memory of the device and write it to flash memory.

Note The system image used depends on your device. For all WAVE and WAE devices (64-bit platforms), use the 64-bit system image (with "x86_64" in its name). For all other devices, use the 32-bit system image named without this designator.

An NPE image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted is provided.

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 WAAS device and open a terminal session.

Step 3 Reboot the device by toggling the power on/off switch.

After a few seconds, the bootloader pauses and prompts you to enter 1 to boot WAAS, r to boot the rescue image, x to reboot, or 9 to escape to the loader prompt. You have 10 seconds to respond before the normal boot process continues.

Step 4 Enter r to boot the rescue image.

The **Rescue Image** dialog box is displayed and differs depending on whether your WAAS device was initially manufactured with Version 4.x or 5.x. Step 5 describes the rescue image on a device that was initially manufactured with Version 5.x. Step 6 describes the rescue image on a device that was initially manufactured with Version 4.x.

Step 5 If you see the following output (from a device that was initially manufactured with Version 5.x), log in and use the **copy install** command to install the WAAS system software image (.bin file), as shown in the following example (user input is denoted by entries in bold typeface):

```
The device is running WAAS rescue image. WAAS functionality is unavailable
in a rescue image. If the rescue image was loaded by accident, please reload
the device. If the rescue image was loaded intentionally to reinstall WAAS software
please use the following command:

    copy [ftp|http|usb] install ...


SW up-to-date
...

Cisco Wide Area Virtualization Engine Console

Username: admin
Password:
System Initialization Finished.

WAVE# copy ftp install 172.16.10.10 / waas-universal-5.1.1.12-k9.bin
...

Installing system image to flash... Creating backup of database content before database
upgrade.
```

```
The new software will run after you reload.
WAVE# reload
Proceed with reload?[confirm]yes
Shutting down all services, will timeout in 15 minutes.
reload in progress ..Restarting system.
```

Step 6 If you see the following output (from a device that was initially manufactured with Version 4.x), log in and install the WAAS system image (.sysimg file), as shown in the following example (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: GigabitEthernet 0/0
    1: GigabitEthernet 0/1
enter choice: 0
Using interface GigabitEthernet 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:

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 (e.g. WAAS-x86_64-4.x.x-K9.sysimg)]:
waas-x86_64-5.1.1.12-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-x86_64-5.1.1.12-k9.sysimg

Attempting download...
Downloaded 31899648 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.
Booting system, please wait.........
```

Step 7 Log in to the device with the username **admin**. Verify that you are running the correct version by entering the **show version** command:

```
Username: admin
Password:

Console# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2012 by Cisco Systems, Inc.
Cisco Wide Area Application Services (universal-k9) Software Release 5.1.1 (buil
d b12 Nov 12 2012)
Version: oe294-5.1.1.12

Compiled 12:23:45 Nov 12 2012 by damaster

Device Id: 50:3d:e5:9c:8f:a5
System was restarted on Mon Nov 12 16:35:50 2012.
System restart reason: called via cli.
The system has been up for 8 hours, 10 minutes, 19 seconds.
```

Recovering a Lost Administrator Password

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

Note You cannot restore a lost administrator password. You must reset the password, 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, and 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 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 passwd** command in global configuration mode:

```
WAE# configure
WAE(config)# username admin passwd
```

This command invokes interactive password configuration. Follow the CLI prompts.

Step 6 Save the configuration change:

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

Step 7 (Optional) Reboot your device:

```
WAE# reload
```

Rebooting is optional. However, we recommend that you 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 automatically by RAID-1 on critical system partitions. Therefore, the procedures in this section do not have to be followed when replacing a disk drive in a multidrive 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 menu, go to **Devices** > *device-name*.

b. Choose *device-name* > **Activation**. The Device Activation window appears.

c. 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.

Install the WAAS software. For more information on initial configuration, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Step 4 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 Recovering WAAS Device Registration Information.

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 Central Manager menu, choose **Devices** > *device-name*.

b. Choose *device-name* > **Activation**.

c. Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.

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

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

Step 2 If the failed device is configured as a nonoptimizing peer with another device, disable the peer settings on the other device.

A message is displayed if the failed device is a nonoptimizing peer, indicating that the device is a nonoptimizing peer. When a device is replaced, its device ID changes and therefore, the nonoptimizing peer configuration must be updated.

a. From the WAAS Central Manager menu, choose **Configure** > **Global** > **Peer Settings**. The Peer Settings window for all the devices appears.

b. Click the **Edit** icon next to the nonoptimizing device identified in the message, which will appear in red because its peer is unknown. The Peer Settings window for that device appears.

c. Click the **Remove Device Settings** icon in the taskbar.

d. Click **Submit**.

Step 3 Configure a system device recovery key as follows:

a. From the WAAS Central Manager menu, choose **Configure** > **Global** > **System Properties**.

b. Click the **Edit** icon next to the System.device.recovery.key property. The Modifying Config Property window appears.

c. Enter the password in the **Value** field, and click **Submit**. The default password is **default**.

Step 4 Configure the basic network settings for the new device.

Step 5 Open a Telnet session to the device CLI and enter the **cms recover identity** *keyword* EXEC command. Here, *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 6 Enter the following commands to enable the CMS service on the device:

```
WAE# config
WAE(config)# cms enable
WAE(config)# exit
```

Step 7 Activate the device:

a. From the WAAS Central Manager menu, choose **Devices** > *device-name*.

b. Choose *Device Name* > **Activation**. The WAAS device status should be Online.

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

Step 8 (Optional) Reconfigure the device peer settings, if the device was configured as a nonoptimizing peer with another device (see Information About Clustering Inline WAEs in Chapter 5, “Configuring Traffic Interception”).

Step 9 Save the device configuration settings by entering the **copy running-config startup-config** EXEC command.

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 and speed 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 a part of the hot-swap process, check for capacity compatibility. Incompatibility generates an alarm and aborts the hot-swap process.

To perform disk maintenance, follow these steps:

Step 1 Manually shut down the disk.

a. Enter global configuration mode and then enter the **disk disk-name** *diskxx* **shutdown** command:

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

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 it is 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 Re-enable the disk by running the **no disk disk-name** *diskxx* **shutdown** global configuration command.

Removing and 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 from the WAAS CLI on the WAE.

Step 2 Verify that the disk drive *diskxx* is in Defunct state by entering the **show disks details** command in EXEC mode. The RAID logical drive is in 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, it means the drive is being accessed.

Note If a disk is shut down using the **disk disk-name diskxx replace** EXEC command and the same disk is removed and reinserted, it can be reenabled by using the EXEC command **disk disk-name diskxx enable force**. This process is applicable even if the disk is not removed and needs to be re-enabled. This command is not applicable if a new disk is inserted.

Step 8 Wait for 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 a 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.

Step 10 Reinstall the software on the device. For more information, refer to Upgrading the WAAS Software

Step 11 Add the license. For more information, refer to Managing Software Licenses in Chapter 10, “Configuring Other System Settings.”

Step 12 Register the WAE to the WAAS Central Manager.

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 re-create the RAID-5 array by following these steps:

Step 1 From the global configuration mode, run the **disk logical shutdown** command to disable the RAID-5 array.

Step 2 Run the **write** command in EXEC mode to save the running configuration to NV-RAM.

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

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

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

Step 6 After successful execution of the **disk recreate-raid** command, enter global configuration mode and run the **no disk logical shutdown** command to disable the logical disk shutdown configuration.

Step 7 Run the **write** command in EXEC mode to save the configuration to NV-RAM.

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

Step 9 Run the **show disks details** command in EXEC mode to check the system configuration after the system is reloaded. 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 running 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.

After a multiple disk failure or RAID controller failure, and after the drives are replaced and the RAID disk is rebuilt, the logical disk may remain in the error state. To re-enable the disk, use the **no disk logical shutdown force** command, and then reload the WAE.

Configuring the Central Manager Role

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 Primary and standby Central Managers communicate on port 8443. If your network includes a firewall between primary and standby Central Managers, you must configure the firewall to allow traffic on port 8443 so that the Central Managers can communicate and stay synchronized.

This section contains the following topics:

- Central Manager Failover and Recovery

Converting a WAE to a Standby Central Manager

This section describes how to convert a WAE that is operating as an application accelerator to a standby Central Manager.

There are two types of WAAS software files:

- Universal—Includes Central Manager, Application Accelerator, and AppNav Controller functionality.
- Accelerator only—Includes Application Accelerator and AppNav Controller functionality only. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must use the Universal software file.

If the WAE is operating with an Accelerator only image, you cannot convert it to a Central Manager until after you update it with the Universal software file, reload the device, change the device mode to central-manager, and then reload the device again. For information on updating a WAE, see Upgrading the WAAS Software.

Use the **show version** EXEC command to check if the WAE is running an Accelerator only image. Also, the **show running-config** EXEC command displays the image type.

To convert a WAE with a Universal image to a standby Central Manager, follow these steps:

Step 1 Deregister the WAE from the Central Manager using the **cms deregister force** command:

```
WAE# cms deregister force
```

This command cleans up any previous association to any other Central Manager.

Step 2 Configure the device mode as Central Manager using the **device mode** command:

```
WAE# configure
WAE(config)# device mode central-manager
```

Step 3 You must reload the device to apply the changes. For more information on reloading and rebooting a device, see Rebooting a Device or Device Group.

Step 4 Configure the Central Manager role as standby using the **central-manager role standby** command:

```
WAE(config)# central-manager role standby
```

Step 5 Configure the address of the primary Central Manager using the **central-manager address** command:

```
WAE(config)# central-manager address cm-primary-address
```

Step 6 Enable the CMS service using the **cms enable** command:

```
WAE(config)# cms enable
```

Converting a Primary Central Manager to a Standby Central Manager

To convert a primary Central Manager to a standby Central Manager, follow these steps:

Step 1 Deregister the Central Manager using the **cms deregister** command:

```
WAE# cms deregister
```

This command cleans up any previous association to any other Central Manager.

Step 2 Configure the Central Manager role as standby using the **central-manager role standby** command:

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

Step 3 Configure the address of the primary Central Manager using the **central-manager address** command:

```
WAE(config)# central-manager address cm-primary-address
```

Step 4 Enable the CMS service using the **cms enable** command:

```
WAE(config)# cms enable
```

Converting a Standby Central Manager to a Primary Central Manager

If your primary WAAS Central Manager becomes inoperable, you can manually reconfigure one of your warm standby Central Managers to be the primary 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 a previous failed primary Central Manager becomes available again, you can recover it to make it the primary Central Manager again. For details, see Central Manager Failover and Recovery.

If you switch a warm standby Central Manager to primary while your primary Central Manager is still online and active, both Central Managers detect each other, automatically shut themselves down, and disable management services. The 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 cm-primary-address
WAE(config)# cms enable
```

Switching Both the Central Manager Roles

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 the current primary Central Manager. 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 the 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. This time range verifies 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 after you configure a role change.

Central Manager Failover and Recovery

If your primary WAAS Central Manager (WAAS CM) becomes inoperable, you can reconfigure one of your standby Central Managers to be the primary Central Manager, and later, when the failed Central Manager becomes available, you can reconfigure it to be the primary again. Follow these steps:

Step 1 Convert a standby Central Manager to be the primary Central Manager, as described in Converting a Standby Central Manager to a Primary Central Manager.

Step 2 When the failed Central Manager is available again, configure it as a standby Central Manager, as described in Converting a Primary Central Manager to a Standby Central Manager, beginning with Step 2. Skip Step 1 and do not use the **cms deregister** command.

Step 3 Switch both the Central Manager roles, as described in Switching Both the Central Manager Roles.

Note In some scenarios, when a Standby Central Manager (SCM) is registered newly with a WAAS Central Manager that is already managing more than 1000 WAEs, the devices may go off line. To avoid this, in case of large deployments, we recommend that you register the SCM to the Primary Central Manager (PCM) at the beginning of the deployment so that in case of an unexpected fail over the SCM takes up the PCM's role.

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 the data in WAAS persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored in 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. After 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 **Devices** > *device-name*, then choose **Configure** > **Storage** > **Disk Encryption**. To enable disk encryption, check the **Enable** check box and click **Submit**. This check 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.

Note If you are using an NPE image, note that the disk encryption feature is disabled in countries where disk encryption is not permitted.

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 provide any service.

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 two 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 can also view the disk encryption status, whether it is enabled or disabled, in the Central Manager GUI's Device Dashboard window.

Configuring a Disk Error-Handling Method

Note Configuring and enabling disk error handling 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.

If the bad disk drive is a critical disk drive, and the automatic reload feature 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.

Note The automatic reload feature is automatically enabled, but is not configurable on devices running WAAS Version 4.1.3 and later.

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

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* **(**or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Storage** > **Disk Error Handling**.

The Disk Error Handling Current Settings window appears.

Step 3 The Disk Error Handling Current Settings window has two check boxes:

- Check the **Enable** check box to enable the window for configuration
- Check the **Enable Disk Error Handling Remap**. This forces the disks to attempt to remap disk errors automatically. This is checked (enabled) by default.

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

Enabling Data Cache Management

The WAAS Central Manager allows you to configure existing Akamai Cache and Object Cache data partitions by increasing or decreasing the cache sizes whenever needed on the existing WAE system. Note the following scenarios with respect to WAAS devices, software version and new or subsequent Data Cache Management configuration.

Upgrading 294,594,694 with software version 6.1.1:

When you upgrade to software version 6.1.1, and configure the device/s for data cache management for the first time and perform a reload.

All the data-cache is lost on reload.

Upgrading vWAAS/ISR-WAAS/SM-SRE with software version 6.1.1:

When you upgrade to software version 6.1.1, and configure the device/s for data cache management for the first time and perform a reload, both data and system partitions are re-created. Logs and Data Cache are cleaned up, but software version and CM registration information is preserved.

Fresh deployment in all models:

When you do a fresh deployment of software version 6.1.1, and configure the device/s for data cache management for the first time and perform a reload, only Akamai and object-cache data is lost.

Second/Subsequent configuration in all models:

Configuring Data Cache Management for second/subsequent times cleans only the Akamai and Object cache partitions. All other partitions are retained.

Limitations

The following limitations for Data Cache Management are applicable:

- If you want to configure data cache management from the WAAS Central Manager GUI, both the WAAS Central Manager and the devices registered with it need to be running version 6.1.1.

- The device needs to be in Application Accelerator mode to configure Akamai and Object Cache capability.
- The Central Manager supports mixed mode of devices in different versions. When you configure Data Cache Management at the Device level, the configurations apply only to the devices running version 6.1.1 and not to those below version 6.1.1.
- Data Cache Management is not supported on the following hardware platforms - 7541, 7571 and 8541, vWAAS 12K and vWAAS 50K.

To enable data cache management using the WAAS Central Manager GUI, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* **(**or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Storage** > **Cache Size Management**.

The Cache Size Management window appears.

Step 3 Select from the available options.

- Default - Sets the available partition size for Akamai cache and Object cache according to predefined values.
- Akamai-Object Cache-Equal - Sets the available partition size to 50% each, for both Akamai cache and Object cache.
- Akamai-weight1- Sets the partition size to 60% for Akamai cache and 40% for Object cache.
- Akamai-weight2 - Sets the partition size to 80% for Akamai cache and 20% for Object cache.
- ObjectCache-weight1 - Sets the partition size to 60% for Object cache and 40% for Akamai cache.
- ObjectCache-weight2 - Sets the partition size to80% for Object cache and 20% for Akamai cache.

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

The data partition is effective only after the device is reloaded.

To enable data cache management the CLI, use the **disk cache enable** global configuration command.

If you want to view the data cache details go to **Devices** >*device-name* **(**or **Device Groups** > *device-group-name*) > **Monitor** > **CLI Commands** > **Show Commands** and select the **show disk cache-details** command. The cache details are displayed for devices that are running version 6.1.1.

Note When you downgrade a device from 6.1.1 to any 5.x.x version, object-cache is no longer valid. As a result the associated clis are also not visible on the devices.

Activating All Inactive WAAS Devices

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

Step 1 From the WAAS Central Manager menu, choose **Devices** > **All Devices**.

The All Devices window appears.

Step 2 Click the **Activate all inactive WAEs** icon in the taskbar.

The Activate All Inactive WAEs window appears.

Step 3 Choose an existing location for all the inactivated WAAS devices by clicking the **Select an existing location for all inactive WAEs** radio button, and then choose a location from the corresponding 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 menu, choose **Devices** > *device-name*.

The device Dashboard appears.

Step 2 Click the **Reload** icon in the Device Info pane.

You are prompted to confirm your decision.

Step 3 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 with user-provided passphrase mode, 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 Central Manager menu, choose **Device Groups** > *device-group-name*.

The Modifying Device Group window appears.

Step 2 In the taskbar, click the **Reboot All Devices in Device Group** icon.

You are prompted to confirm your decision.

Step 3 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 Guide*.

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*.

Limitations of a Controlled Shutdown

After the devices has been registered to the WAAS Central Manager (WAAS CM), a WCM DB VACUUM (runs between 1 a.m. to 2 a.m.) process takes more time (Min:2 min, Avg:7 min, Max:25min) due to known issues in the WAAS CM.

- Few of the WAEs may go temporarily offline. They are online automatically once the VACUUM process is complete.
- Statistics Aggregation threads may take more than 5 minutes and the same is indicated in the logs. As a result, statistics samples, might be missing at network level.
- Users, including the administrator, will not be able to use (log in to) the WAAS CM because the complete DB will be locked.