



Release Note for Cisco Wide Area Application Services Software Version 4.0.23

July 17, 2009



Note

The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note applies to Cisco Wide Area Application Services (WAAS) software version 4.0.23. For information on WAAS features and commands, see the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.



Note

If you are running version 4.0.21 or earlier, we recommend that you upgrade to version 4.0.23 at your earliest convenience.

This release note contains the following sections:

- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.23](#)
- [Upgrading from Version 4.0.x to 4.0.23](#)
- [Downgrading from Version 4.0.23 to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade](#)
- [Cisco WAE-612 Hard Disk Drive Replacement Notification](#)
- [Operating Considerations](#)
- [Software Version 4.0.23 Resolved Caveats](#)
- [Software Version 4.0.23 Open Caveats](#)
- [WAAS Documentation Set](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2009 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation and Submitting a Service Request](#)

Upgrading From WAFS to WAAS

Although WAFS to WAAS migration is supported, a rollback from WAAS to WAFS is not supported. For information regarding a WAFS-to-WAAS migration, contact your Cisco Sales Engineer.

If you are upgrading from WAFS 3.0.7 or later to WAAS, you must upgrade to WAAS version 4.0.x only; you cannot upgrade to a prerelease version of 4.0.x.

If you are upgrading from the WAFS 3.0.7-special5 build or from a later WAFS release to WAAS, we recommend that you upgrade to the most current version of WAAS to ensure that you obtain all of the latest fixes and features. (You must upgrade to a minimum of WAAS 4.0.5 or later.)

Note the following points when upgrading from WAFS to WAAS:

- When you upgrade from WAFS to WAAS, you may lose up to half of the WAFS cache space because the upgrade process uses the WAFS cache eviction process to reclaim the space needed for the DRE cache; the oldest content is removed first.
- The hardware that supports WAFS 3.0 also supports WAAS, with the exception of the NM-CE.
- You need a dedicated WAE to function as the Central Manager in WAAS.
- You must place the WAEs in a separate subnet from the clients, or you must use the GRE return feature.

Upgrading from a Prerelease Version to Version 4.0.23

To upgrade from WAAS prerelease software to version 4.0.23, you must perform one of the following tasks to ensure a successful upgrade:

- Restore the factory default settings by using the **restore factory-default** command.
- Perform a fresh install from the rescue CD.

Upgrading from Version 4.0.x to 4.0.23

This section contains the following topics:

- [Requirements and Guidelines](#)
- [Running the WAAS Disk Check Tool](#)
- [Ensuring a Successful RAID Pair Rebuild](#)
- [Managing Passwords after an Upgrade](#)

Requirements and Guidelines

When you upgrade from version 4.0.x to version 4.0.23, observe the following guidelines and requirements:

- To take advantage of bug fixes and new features, we recommend that you upgrade your entire WAAS deployment to the latest version.

- Before you upgrade your WAE from version 4.0.3 or earlier, you may need to run a script (the WAAS disk check tool) to check the file system for errors that may result from a RAID synchronization failure. See the “[Running the WAAS Disk Check Tool](#)” section on page 3. 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.
- Upgrade the WAE devices first, and then upgrade the WAE Central Manager devices.
- If you operate a network with devices that have different software versions, the WAAS Central Manager must be the lowest version.
- WAAS version 4.0.23 supports strong passwords. When you upgrade from an earlier version that does not support strong passwords, the previous weaker passwords will be retained. For details, see the “[Managing Passwords after an Upgrade](#)” section on page 5.
- When you upgrade WAAS devices to version 4.0.23 from version 4.0.17 or earlier, the EPM classification feature is disabled and removed from the CLI and Central Manager GUI. If you use a WAE running WAAS 4.0.23 with an older Central Manager that supports EPM, the WAE will ignore any EPM configuration commands issued by the Central Manager. Also, the **show running-config** command on an upgraded WAE may show the EPM dynamic map, but it has no effect on system operation.
- When you upgrade the Central Manager to version 4.0.23, the CIFS-non-wafs classifier is removed from edge and core devices automatically. (This classifier was removed in version 4.0.7.)
- When you upgrade edge and core devices to version 4.0.23, the CIFS-non-wafs classifier remains. If your Central Manager is operating at a lower version, you must manually delete the CIFS-non-wafs classifier and its policy map.

To delete the CIFS-non-wafs classifier using the Central Manager GUI, follow these steps:

1. Choose **Devices > Devices** (or **Device Groups**) > **Acceleration > Policy Definitions**.
2. Click the **Edit** icon next to the CIFS-non-wafs policy.
3. Click **Edit Classifier**. The Modifying Application Classifier window appears.
4. To delete the classifier and its policy, click the **Trash** icon.

Running 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 may result from a RAID synchronization failure. (For more information, see the “[Ensuring a Successful RAID Pair Rebuild](#)” section on page 4.) 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 may obtain the WAAS disk check tool from the following URL:

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

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.

To run the WAAS disk check tool, follow these steps:

Step 1 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
```

Step 2 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
```

Step 3 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
```

Step 4 If a file system contains errors, follow the instructions in the `disk_status.txt` file to repair the file system.

Ensuring a Successful RAID Pair Rebuild

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.



Caution

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.

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** command in EXEC mode. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process may 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 that could indicate a problem:

- The device is offline in the Central Manager GUI.
- CMS cannot 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,” or “ext3_readdir: bad entry in directory.”
- Other unusual behaviors occur that are 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. (For information about obtaining and using this tool, see the [“Running the WAAS Disk Check Tool”](#) section on page 3.)

Managing Passwords after an Upgrade

WAAS software version 4.0.23 includes a strong password feature for improved security. WAAS software version 4.0.21 and 4.0.19 also support the strong password capability. WAAS software version 4.0.17 and earlier do not have a strong password capability.



Note

The following considerations apply to WAAS software version 4.0.23 (and versions 4.0.19 and 4.0.21) with the strong password policy enabled. Strong passwords are disabled by default.

When you upgrade from a previous version to version 4.0.23 please note the following password considerations:

- Existing passwords from the older version will continue to work in version 4.0.23.
- Existing passwords will expire after 90 days. Subsequent new passwords must conform to strong password requirements.
- Strong passwords must meet the following requirements:
 - The password must be at least 11 characters long.
 - The password can include both uppercase and lowercase letters (A–Z and a–z), numbers (0–9), and special characters including ~`!@#%&*()_+=[\] ; : , < / > .
 - The password cannot contain all the same characters (for example, 99999).
 - The password cannot contain consecutive characters (for example, 12345).
 - The password cannot be the same as the username.

Downgrading from Version 4.0.23 to a Previous Version

If you enable disk encryption in version 4.0.23 and then downgrade to a software version that does not support this feature (4.0.11 or earlier), you will not be able to use the disk partitions. In such cases, you must delete the disk partitions after you downgrade.

If you enable features such as secure storage and strong passwords in version 4.0.23, you must disable them before you downgrade WAAS to version 4.0.17 or earlier.

Locked-out user accounts will be reset upon downgrade.

This section contains the following topics:

- [Downgrading to Version 4.0.21, 4.0.19, 4.0.17, or 4.0.13](#)
- [Downgrading to Version 4.0.11 or Earlier](#)

**Note**

When you downgrade from version 4.0.23 to a previous version, any features or configuration settings that are not supported by the previous version will be lost.

Downgrading to Version 4.0.21, 4.0.19, 4.0.17, or 4.0.13

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.0.21, 4.0.19, 4.0.17, or 4.0.13, follow these steps:

-
- Step 1** Disable secure storage mode if it is enabled by using the `cms secure-store clear` global configuration command. (This step is not required when downgrading to version 4.0.21 or 4.0.19.)
- Step 2** Disable the management service by using the `no cms enable` global configuration command.
- ```
(config)# no cms enable
```
- Step 3** From the Central Manager CLI, create a database backup by using the `cms database backup` EXEC command. Move the backup file to a separate device.
- ```
CentralManager# cms database backup
```
- Step 4** Install the 4.0.x image by using the `copy ftp install` EXEC command.
- Step 5** Reload the device.
- The database needs to be downgraded before the Central Manager can use it and the CMS process can start. To optionally verify this status, use the `show cms info` EXEC command. It should respond with a message saying that a database downgrade is required.
- Step 6** Downgrade the database by using the `cms database downgrade` EXEC command.
- ```
CentralManager# cms database downgrade
```
- Step 7** Enable the CMS service by using the `cms enable` global configuration command.
- ```
config
(config)# cms enable
```
-

Downgrading the database may trigger full updates for registered devices. In the Central Manager GUI, ensure that all previously operational devices come online.

Downgrading to Version 4.0.11 or Earlier

**Note**

A pre-4.0.13 CMS database backup is required for this procedure.

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.0.11 or earlier, follow these steps:

-
- Step 1** Disable secure storage mode if it is enabled by using the `cms secure-store clear` global configuration command.
- Step 2** Disable the management service by using the `no cms enable` global configuration command.
- ```
(config)# no cms enable
```

**Step 3** From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command.

```
CentralManager# cms database backup
```

**Step 4** Install the pre-4.0.13 image by using the **copy ftp install** EXEC command.

**Step 5** Reload the device.

**Step 6** After the device reloads, enter the **cms database delete** EXEC command.

```
CentralManager# cms database delete
```

This command deletes and reinitializes the internal database files and restarts the database service.

**Step 7** Initialize the CMS database tables by using the **cms database create** EXEC command.

```
CentralManager# cms database create
```

**Step 8** On the Central Manager, restore the pre-4.0.13 CMS database backup, if available.

```
CentralManager# cms database restore <pre-4.0.13-db-backup>
```

**Step 9** Enable the CMS service by using the **cms enable** global configuration command.

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

## Cisco WAE and WAVE Appliance Boot Process

To monitor the boot process on Cisco WAE and WAVE appliances, connect to the serial console port on the appliance as directed in the *Hardware Installation Guide*.

Cisco WAE and WAVE appliances have video connectors that should not be used in normal operation. The video output is for troubleshooting purposes only during BIOS boot and stops displaying output as soon as the serial port becomes active.

## Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade

Under rare circumstances, the RAID controller firmware used in the WAE-674, WAE-7341, and WAE-7371 appliances can cause the disk storage subsystem to go offline and the affected devices to stop optimizing connections. The symptoms are as follows:

- Syslog output contains several instances of the following message:  
“WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device.”

- A sysreport and running-config cannot be generated and copied to /local/local1.

Both of the above symptoms are an indication of the file system becoming read-only during traffic flow.

- An increasing number of pending connections appear in the output of the **show statistics tfo** command, indicating that new connections cannot be optimized. You can use this command to proactively check the functionality of the system.

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on cisco.com at the [Cisco Wide Area Application Engine \(WAE\) Utilities Software Downloads \(registered customers only\)](#) page. The firmware binary image is named L4\_15427\_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware and are named L4\_15427\_FIRMWARE.pdf.

## Cisco WAE-612 Hard Disk Drive Replacement Notification

This notice applies to the WAE-612 and all WAAS versions previous to 4.0.19 that support the hot-swap replacement of drives while the appliance is running.

A problem may occur while replacing the drives while the unit is running. Occasionally after a drive hot-swap procedure, the WAE-612 may stop operating and require a reboot.

To avoid this problem, upgrade your WAAS software to version 4.0.19 or later.

This notice does not apply to the WAE-674, WAE-7341, or WAE-7371. .

## Operating Considerations

This section includes operating considerations that apply to software versions 4.0.23:

- [Using Autoregistration with Port-Channel Interfaces](#)
- [WAFS Support of FAT32 File Servers](#)
- [Running the File Server Rename Utility](#)

### Using Autoregistration with Port-Channel Interfaces

Do not enable the **auto-register** global configuration command when both interfaces are configured as port-channel interfaces.

### WAFS Support of FAT32 File Servers

The WAFS feature does not support file servers that use the FAT32 file system. You can use the policy engine rules to exclude from CIFS optimization any file servers that use the FAT32 file system.

### Running the File Server Rename Utility

The File Server Rename tab enables you to change the resource location for all resources of a given file server name, on the WAFS Edge device. The files are renamed in the WAFS cache. When you run the file server rename utility, be sure you do not rename the file server with the same name as another existing file server. Assigning an existing name to a file server will overwrite the file server's contents.

## Software Version 4.0.23 Resolved Caveats

The following caveats were resolved in software version 4.0.23:

| Caveat ID Number           | Description                                                            |
|----------------------------|------------------------------------------------------------------------|
| <a href="#">CSCsw23717</a> | Under rare conditions WAE may generate a dataserver core file.         |
| <a href="#">CSCsy05336</a> | Client GUI connection to Print Services Admin may return error page.   |
| <a href="#">CSCsy70855</a> | WAE may generate a dataserver core file for a WAFS statistics request. |

## Software Version 4.0.23 Open Caveats

The following open caveats apply to software version 4.0.23:

- **CSCsk41815**—The /local/local1 (SYSFS) partition runs out of space when TFO transaction logging is enabled and a lot of traffic going through the WAE device. TFO transaction logs are normally removed after two days, but if a large number of connections occur in one day, they can fill up the disk. Workaround: Either disable the TFO transaction logging or remove the log files manually.
- **CSCsl56564**—The “not in repository” message is shown for the printer drivers after the standby Central Manager becomes the primary Central Manager. This error occurs because the printer driver files are removed from the repository. Workaround: Copy the tdb files that are stored in the /var/lib/samba directory of the primary Central Manager to the standby Central Manager before switching it to the primary Central Manager. Use the **windows-domain diagnostics tdb-list** command to list the tdb files and use the **windows-domain diagnostics tdb-move** to move the tdb files.
- **CSCso16224**—If a WAE is configured for Windows authentication but is not registered to the Windows domain, a winbindd core file is generated. Workaround: Register the WAE to the Windows domain.
- **CSCso37013**—When you are using WAFS, CIFS traffic performance may be negatively affected. In extreme cases, the Core WAE may reboot. This situation occurs because of slow reverse-DNS lookup. Workaround: Correct the reverse DNS problems in your network, or disable reverse DNS on the Core WAE using the CLI command **show stat wafs expert “-server Tx -mbean CIFSserversConfig -attr UseReverseDNS false”**.
- **CSCsq02282**—The connection list in the WAAS CLI does not match the connection list in the Central Manager GUI. Workaround: Navigate to **Device > Monitoring > Connections Statistics** and click the **Refresh** button at the bottom of the table to update the display of the connection statistics. Or use the CLI to get the correct list of active connections on the network.
- **CSCsq29189**—When you downgrade or roll back a WAE device to a previous software version, you receive the error message: “Roles changed, reload required.” Workaround: Reload the software again to clear the alarm.
- **CSCsq43732**—The network analysis tool tethereal malfunctions while attempting to capture certain packet types from the WAE device. This situation does not affect WAAS system operation. Workaround: Restart tethereal and retry the packet capture.
- **CSCsq58639**—When you upgrade to version 4.0.19 and then enable secure store on the WAE device, the TFO policies are listed as being in the override state. Workaround: On the Policy Definitions page, click the Force Device Group button to reapply the policy settings.

- **CSCsr07423**—When you use Windows Explorer to browse a file server optimized by WAAS, the Summary tab for file properties may display empty fields. (Right click on any file, select Properties, and then select the Summary tab.) Workaround: If the summary information fields are empty, run the CLI command **show stat wafs expert "-server Rx -mbean RxCIFS -attr LocallyDeniedStreamPattern .+:Docf\_\092005.+"**.
- **CSCsu75417**—A core file is created for a specific Java event. This situation occurs when “killall -QUIT java” is called while the CMS process is just starting. Workaround: None.
- **CSCsv33344**—Clients from unoptimized sites are randomly unable to connect to servers. This situation occurs with multiple WCCP routers and WAEs in a farm. The WCCP flow tables are mismatched for WCCP service 61 & 62. Workaround: The WCCP farm reconfiguration can potentially clear up the incorrect states. Removing and re-adding the concerned WAE from the farm using the commands **no wccp version 2** and **wccp version 2** can rectify the WCCP flow tables.
- **CSCsv42901**—The primary Central Manager becomes unresponsive and incorrectly indicates that WAE devices are inactive. This situation occurs under heavy load while the primary Central Manager is beginning to update the standby Central Manager. Workaround: Disable the CMS process on the standby Central Manager. Manually make CMS database backups when changes are made or WAE devices are added to the CM.
- **CSCsv65297**—When your Windows98 clients send print traffic to a Windows2003 central print server over WAAS, a delay of several minutes may occur when going through WAFS. The delay is not seen with Windows XP clients. Workaround: None.
- **CSCsv84280**—When you use the CPU statistics graph in the WAAS Central Manager, the custom settings for the graph do not work. Workaround: Use standard settings for the CPU statistics graph.
- **CSCsw86260**—SCSI subsystem alarm gets cleared automatically after 30 minutes when RAID alarm is cleared. Workaround: Configure disk error handling reload to threshold 1.
- **CSCsw82153**—When upgrading a device, CIFS Statistics/Graphs on the CM/Device GUI are seen only since boot-up and statistics that occurred before the upgrade are lost. The CPU and disk statistics at the device GUI are also lost after the upgrade. Workaround: None.

## WAAS Documentation Set

In addition to this document, the WAAS documentation set includes the following publications:

- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *Installing the Cisco WAE Inline Network Adapter*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

