Release Note for Cisco Wide Area Application Services

February 11, 2011

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 versions 4.0.15 and 4.0.17. 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 Software version 4.0.15 is no longer available for download. To upgrade your WAAS software, use software version 4.0.17 or greater.

Note If you are running version 4.0.15 we recommend that you upgrade to version 4.0.17 at your earliest convenience.

This release note contains the following sections:

- WAAS Product Overview
- New Features
- Configuring IP Addresses on the Cisco WAE Inline Network Adapter Interfaces
- New Wide Area Application Engine Supported
- Upgrading From WAFS to WAAS
- Upgrading from a Prerelease Version to Version 4.0.15 or 4.0.17
- Upgrading from Version 4.0.x to 4.0.15 or 4.0.17
- Downgrading from Version 4.0.15 or 4.0.17 to a Previous Version

---

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

- Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade
- Cisco WAE-612 Hard Disk Drive Replacement Notification
- Operating Considerations
- Documentation Enhancements and Corrections
- Software Version 4.0.17 Open Caveats, and Resolved Caveats
- Software Version 4.0.15 Open Caveats, Resolved Caveats, and Command Changes
- WAAS Documentation Set
- Obtaining Documentation and Submitting a Service Request

WAAS Product Overview

The WAAS system consists of a set of devices called Wide Area Application Engines (WAEs) that work together to optimize TCP traffic over your network. When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs to act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

You may use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You may also use the WAAS Central Manager GUI to create new application policies so that the WAAS system will optimize custom applications and less common applications.

Cisco WAAS helps enterprises meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
  - Low data rates (constrained bandwidth)
  - Slow delivery of frames (high network latency)
  - Higher rates of packet loss (low reliability)

New Features

WAAS software versions 4.0.15 and 4.0.17 include the following new features and changes:

- Supports configuring IP addresses on the interfaces on the Cisco WAE Inline Network Adapter and making an inline interface the primary interface on the WAE. For more information, see the "Configuring IP Addresses on the Cisco WAE Inline Network Adapter Interfaces" section on page 3.

- Provides a new troubleshooting facility through the **test** CLI command. For more information, see the "test" section on page 28.

- Provides an enhanced setup utility that runs when a WAAS device first boots. The setup utility can also be accessed via the **setup** EXEC command. Setup utility enhancements include the following:

  - Configuring the device mode (central manager or application accelerator)

  - Configuring the WAE for WCCP or inline interception

  - Configuring a router list for WCCP interception

  - Configuring the inline group identifier, interface speed, and duplex mode for the inline adapter

  - Configuring the primary interface of the WAE (including the inline group interfaces)

  - Configuring an NTP server and time zone

- Supports the new WAE-674 appliance. For more information, see the "New Wide Area Application Engine Supported" section on page 8.

- Provides a new option on the software recovery CD-ROM installer menu for the WAE-674, WAE-7341, and WAE-7371 devices: Option 8: Recreate RAID device. Choosing this option causes the device to recreate the RAID array.

- The Endpoint Port Mapper (EPM) Classification (EPM adapter) feature has been disabled in WAAS 4.0.15 and 4.0.17. It has been removed from the CLI and the WAAS Central Manager GUI. Optimization and acceleration functionality are not affected. To achieve the same monitoring result as was provided by EPM Classification, you can create new application policies to monitor Microsoft Exchange Server traffic, based on the IP addresses of the Exchange servers.

- New commands have been added for WAAS 4.0.15 and 4.0.17. For details see the "Software Version 4.0.15 New and Changed Commands" section on page 27.

Configuring IP Addresses on the Cisco WAE Inline Network Adapter Interfaces

The WAAS 4.0.15 and 4.0.17 releases provide support for configuring IP addresses on the inline interfaces of the Cisco WAE Inline Network Adapter. Also, an inline group interface can be set as the primary interface on the WAE.

When you use the Cisco WAE Inline Network Adapter in your network, you can use the inline interfaces for both management traffic and inline interception. In this case, there is no need to use the Ethernet interfaces that are built into the WAE device.
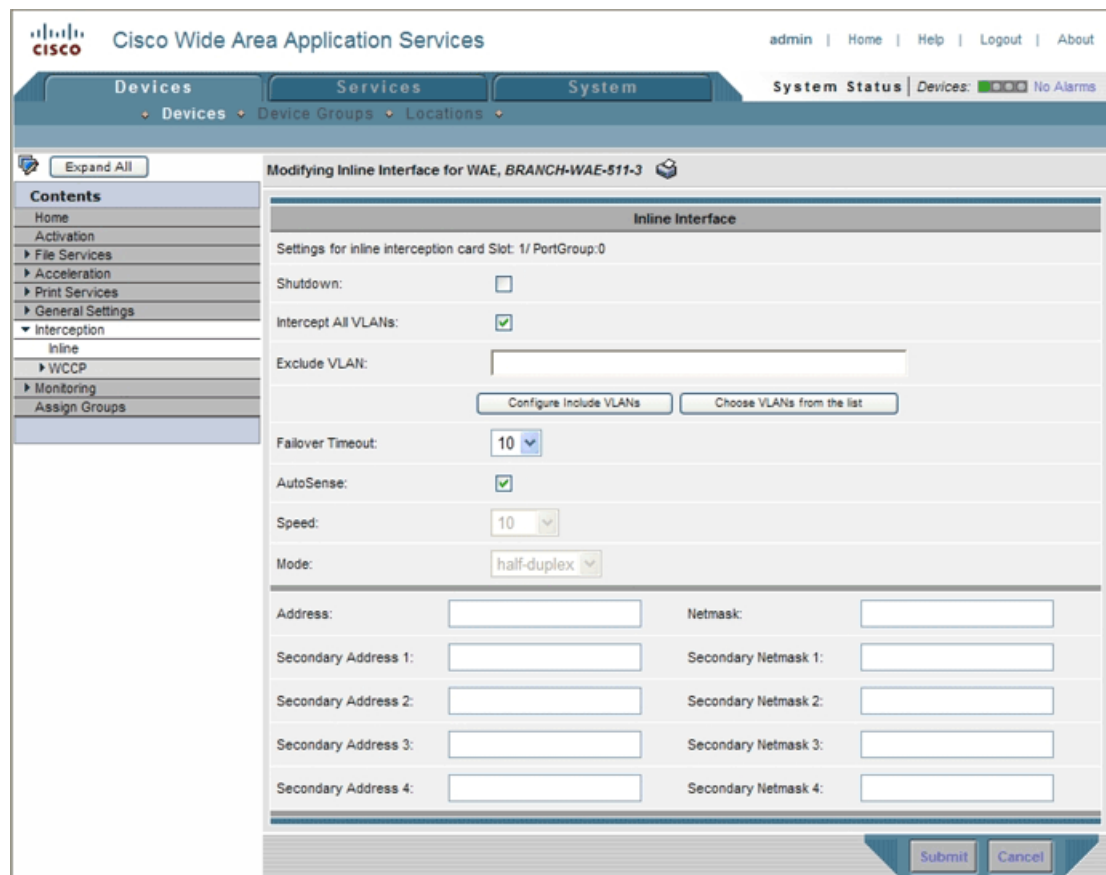
This section contains the following topics:

- Configuring an Inline Interface from Central Manager, page 4

- Configuring an Inline Interface from the CLI, page 6

- Operating Considerations, page 7

Configuring an Inline Interface from Central Manager

To configure an IP address on an inline interface group in the WAAS Central Manager, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**. (You cannot configure inline interface settings from Device Groups.)

The Devices window appears, listing all the device types configured in the WAAS network.

Step 2 Click the **Edit** icon next to the device for which you want to modify the inline settings.

The Device Home window appears with the Contents pane on the left.

Step 3 In the Contents pane, choose **Interception > Inline**.

The Inline Interfaces window appears, listing the inline interface groups available on the device. Click the **Edit Inline Interface** icon next to the inline interface group that you want to modify.

The Modifying Inline Interface window appears, displaying the inline interface configurations for a particular slot and group. (See Figure 1.)

Figure 1   Modifying Inline Interfaces Window

Step 4 In the lower part of the screen, in the Address field, enter an IP address for the inline interface.

Step 5 In the Netmask field, enter a subnet mask for the inline interface.

Step 6 (Optional) Enter up to four secondary IP addresses and corresponding subnet masks in the Secondary Address and Secondary Netmask fields.

Step 7 Configure other settings as described in Chapter 4 of the *Cisco Wide Area Application Services Configuration Guide*.

In the upper part of the window, one new button was added in versions 4.0.15 and 4.0.17: **Configure Include VLANs**. Click this button when you know the list of VLANs that you want to include in inline interception. This button runs a script that prompts you for a comma-separated list of VLANs that you want to include. The script generates an inverse list of all VLANs that should be excluded and then updates the window and puts the list into the Exclude VLAN field.

Step 8 Click **Submit**.

To set an inline interface as the primary interface on a WAE, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**. (You cannot configure network settings from Device Groups.)

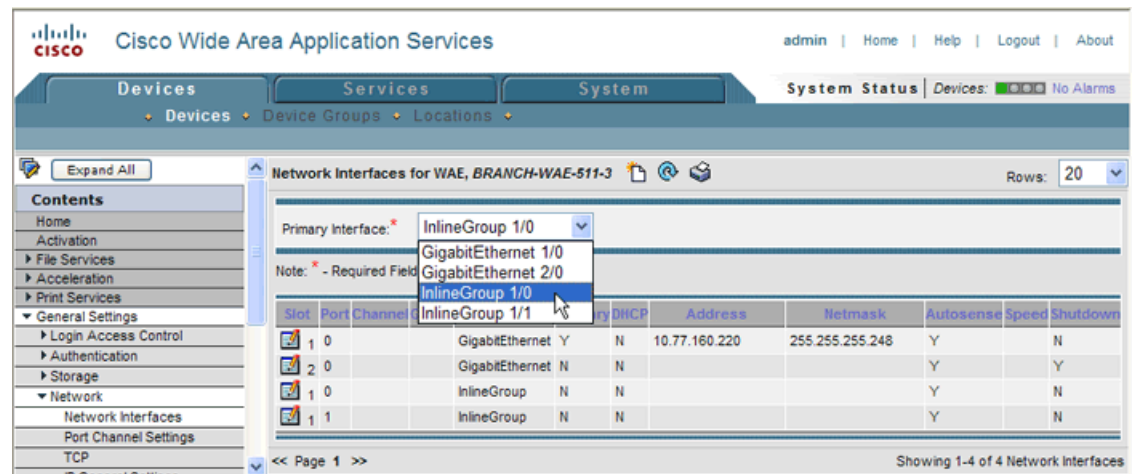The Devices window appears, listing all the device types configured in the WAAS network.

Step 2 Click the **Edit** icon next to the device for which you want to modify the network settings.

The Device Home window appears with the Contents pane on the left.

Step 3 In the Contents pane, choose **General Settings > Network > Network Interfaces**.

The Network Interfaces window appears, listing the interfaces available on the device, as shown in Figure 2.

Figure 2   **Network Interfaces Window**

Step 4 To set an inline interface group as the primary interface, choose the inline group from the Primary Interface drop-down list.

You are prompted to confirm the change of primary interface. Click **OK** to change the primary interface or **Cancel** to cancel the change.

In scenarios where the primary interface for a WAE is set to an inline group interface and management traffic is configured on a separate IP address (either on a secondary IP address on the same inline group interface or on a built-in interface), you must configure the WAAS Central Manager to communicate with the WAE on the IP address designated for management traffic. Configure the WAE management traffic IP address in the **Devices > Device > Activation** window, in the Management IP field.

Configuring an Inline Interface from the CLI

To configure IP addresses on an inline interface from the CLI, use the **ip** interface configuration command, which has been enhanced to support IP configuration on inline interfaces:

```
(config)# interface inlineGroup 1/0
(config-if)# ip address 10.10.10.10 255.255.255.0
```

You can also set secondary IP addresses for the inline interface, by using the **secondary** option, as follows:

```
(config-if)# ip address 10.10.22.30 255.255.255.0 secondary
```

If a WAE with the Cisco WAE Inline Network Adapter is present in an 802.1Q VLAN trunk line between a switch and a router, and you are configuring the inline interface with an IP address, you must set the VLAN ID that is to be assigned to traffic that leaves the WAE. The VLAN ID should be set to match the VLAN ID expected by the router.

Use the new **encapsulation dot1Q** interface command to assign a VLAN ID, as follows:

```
(config)# interface inlineGroup 1/0
(config-if)# encapsulation dot1Q 100
```

This example shows how to assign VLAN ID 100 to the traffic leaving the WAE. The VLAN ID can range from 1 through 4094.

> **Note** You must use the **encapsulation dot1Q** interface command if you want to set the VLAN ID of the inline traffic. You cannot configure this setting through the WAAS Central Manager.
>
> If the VLAN ID that you set with the **encapsulation dot1Q** interface command does not match the VLAN ID expected by the router subinterface, you may not be able to connect to the inline interface IP address.
>
> The inline adapter supports only a single VLAN ID for each inline group interface. If you have configured a secondary address from a different subnet on an inline interface, you must have the same secondary address assigned on the router subinterface for the VLAN.

To make an inline interface the primary interface on a device, use the **primary-interface** command, which has been enhanced to support setting an inline interface as the primary interface:

```
(config)# primary-interface inlineGroup 1/0
```

To show inline interface IP address information, use the **show interface** command, which has been enhanced to show IP address information for inline interfaces:

```
# show interface inlineGroup 1/0
```

The IP addresses for the inline interface are internally assigned to the WAN side of the group pair, so the IP address information is reported only for the WAN port in the command output.

Operating Considerations

The following operating considerations apply to configuring IP addresses on the inline interfaces:

- This feature provides basic routable interface support and does not support the following additional features associated with the built-in interfaces: standby, port channel, and Cisco Discovery Protocol (CDP).

- If you have configured a WAE to use the inline interfaces for all traffic, inline interception must be enabled or the WAE will not receive any traffic.

- If you have configured a WAE to use the inline interfaces for all traffic and it goes into mechanical bypass mode, the WAE become inaccessible through the inline interface IP address. Console access is required for device management when an inline interface is in bypass mode.

- If you have configured a WAE with an IP address on an inline interface, the interface can accept only traffic addressed to it and ARP broadcasts, and the interface cannot accept multicast traffic.

- In a deployment using Hot Standby Router Protocol (HSRP) where two routers that participate in an HSRP group are directly connected through two inline groups, HSRP works for all clients if the active router fails. However, this redundancy does not apply to the IP address of the WAE itself for management traffic if management traffic is also configured to use the inline interface. If the active router fails, you will not be able to connect to the WAE inline IP address because the inline interface is physically connected to the failed router interface. You will be able to connect to the WAE through the second inline group interface that is connected to the standby router. If redundancy is needed for the IP address of the WAE itself for management traffic, we recommend that you use the IP addresses of the built-in interfaces rather than the inline interfaces.

- If you have configured a WAE to use the inline interfaces for all traffic and have not assigned IP addresses to the built-in interfaces, and then you downgrade the WAE to a version prior to 4.0.15, internal services on the WAE that are using the IP address assigned to the inline interface will lose connectivity. Before downgrading the WAE, configure the built-in interfaces with the appropriate network settings.

- Configuring IP addresses on the inline interfaces in a WAE is not supported if the WAAS Central Manager is running a software version prior to 4.0.15, even if the WAE is running version 4.0.15 or later.

- If you downgrade the WAAS Central Manager to a version prior to 4.0.15, in a deployment where a WAE is configured to use the inline interfaces for all traffic, the WAAS Central Manager will lose communication with the WAE because it cannot recognize the inline interface as the primary interface. To avoid losing communication, either configure the WAE to accept management traffic on one of the built-in interfaces, or set the inline interface IP address as the alternate management address in the **Devices > Device > Activation** window, in the Management IP field.

New Wide Area Application Engine Supported

The WAAS 4.0.15 and 4.0.17 releases introduce support for a new Wide Area Application Engine (WAE) appliance, the WAE-674. The WAE-674 appliance is recommended for edge deployments at medium and large-sized enterprise branch offices and for core deployments at small and medium-sized data centers.

The WAE-674 appliance is described in the following sections:

- Features and Benefits
- New and Changed Commands for the WAE-674 Platform

Features and Benefits

The WAE-674 appliance provides the following features and benefits:

Feature	Benefit
Hardware RAID-5	Allows the appliance to continue operating with one drive in a nonfunctioning state for increased reliability. Provides increased logical disk capacity.
Disk hot-swap capability	No downtime when removing or installing hard disk drives.
64-bit kernel	Allows increased memory capacity for high performance, multi-service operation.
300-GB SAS[1] hard disk drives	3 × 300 GB, RAID-5 configuration
Disk monitoring	Allows you to monitor, analyze, and control the RAID status through the CLI and view basic disk status in the RAID from the Central Manager GUI.
Redundant, hot-swap power supply upgrade option	No downtime when replacing a power supply.

1. SAS = Serial Attached SCSI

The WAE-674 can be configured with either 4 GB or 8 GB of memory.

New and Changed Commands for the WAE-674 Platform

The new WAE-674 supports the same disk commands that were added in release version 4.0.13.23 for the WAE-7341 and WAE-7371 devices.

Table 1 lists commands that were added in the WAAS 4.0.13.23 release to these platforms. These commands also apply to the WAE-674.

Table 1   CLI Commands Added in Version 4.0.15 for WAE-674

Mode	Command and Syntax	Description
EXEC	show disks tech-support	Displays all available information from the RAID controller, including the disk status (logical and physical), the disk vendor ID, and serial numbers. On other WAEs, this command replaces the **show disk smart-info** EXEC command.
	disk disk-name *diskxx* replace	Shuts down the disk for removal.
	disk recreate-raid	Removes the logical drive from the RAID-5 array and then recreates the RAID array. All data contained in the logical drive will be lost. The operation of this command results in synchronizing all drives. While the drives are synchronizing, the system remains operational, but the performance will be slower.
Global configuration	disk logical shutdown	Shuts down the RAID-5 array.

Table 2 lists existing commands that were modified in the WAAS 4.0.13.23 release to support the WAE-7341 and WAE-7371 devices. These modifications also apply to the WAE-674.

Table 2   CLI Commands Modified in Version 4.0.15 for WAE-674

EXEC	disk scan-errors	This command is now available on the logical drive for the WAE-674. The syntax of the existing command was modified for RAID-5 systems; the *diskname* option was removed. The functionality remains the same.
	disk delete-partitions	This command is now available on the logical drive for the WAE-674. This command deletes the entire logical RAID-5 volume. The syntax of the existing command was modified for RAID-5 systems; the *diskname* option was removed. The functionality remains the same. On the next reboot, if the RAID array is still identified as good, the partition table will be recreated and all partitions will be initialized, during which time, the system will not process any traffic.

Table 3 lists a command that was removed for the WAE-7341 and WAE-7371 in the WAAS 4.0.13.23 release. This command is also not available on the WAE-674 but is still available on other supported WAE hardware platforms.

Table 3   CLI Commands Removed in Version 4.0.15 for WAE-674

Mode	Command and Syntax	Description
EXEC	show disks failed-sectors	Failed disk sectors are monitored internally by the RAID controller.

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 a release version of WAAS 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, you must upgrade to a minimum of WAAS 4.0.5 or later; however, to ensure that you obtain all of the latest fixes and features, we recommend that you upgrade to the most current release of WAAS.

Note the following points regarding upgrading from WAFS to WAAS:

- When you upgrade from WAFS to WAAS, up to half of the WAFS cache space may be lost. 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 will also support WAAS, with the exception of the NM-CE.
- You will need a dedicated WAE to function as the Central Manager in WAAS.
- The WAEs will need to be placed in a separate subnet from the clients, or you will need to use the GRE return feature.

Upgrading from a Prerelease Version to Version 4.0.15 or 4.0.17

To upgrade from WAAS prerelease software to version 4.0.15 or 4.0.17, 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 4.0.15 or 4.0.17

This section contains the following topics:

- Requirements and Guidelines
- Running the WAAS Disk Check Tool
- Ensuring a Successful RAID Pair Rebuild

Requirements and Guidelines

When you upgrade from version 4.0.x to version 4.0.15 or 4.0.17, observe the following guidelines and requirements:

- To take advantage of bug fixes and new features, we recommend that you upgrade your entire deployment to the latest software release.
- Before you upgrade your WAE from version 4.0.3 or earlier, you may need to run a script (the WAAS disk check tool) that checks the file system for errors that may result from a RAID synchronization failure. See the "Running the WAAS Disk Check Tool" section on page 11. 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.
- When you upgrade WAAS devices to version 4.0.15 or 4.0.17, the EPM classification feature is disabled and removed from the CLI and Central Manager GUI. If a WAE with WAAS 4.0.15 or 4.0.17 is being used 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.
- When you upgrade the Central Manager to version 4.0.15 or 4.0.17, 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 4.0.15 or 4.0.17, 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:

Step 1 Choose **Devices > Devices** (or **Device Groups**) **> Acceleration > Policy Definitions**.

Step 2 Click the **Edit** icon next to the CIFS-non-wafs policy.

Step 3 Click **Edit Classifier**. The Modifying Application Classifier window appears.

Step 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 12.) 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 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 11.)

Downgrading from Version 4.0.15 or 4.0.17 to a Previous Version

If you enable disk encryption in version 4.0.15 or 4.0.17 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.

Downgrading to Version 4.0.13

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

Step 1 Disable the management service by using the **no cms enable** global configuration command.

```
(config)# no cms enable
```

Step 2 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 3   Install the 4.0.13 image by using the **copy ftp install** EXEC command.

Step 4   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 5   Downgrade the database by using the **cms database downgrade** EXEC command.

```
# cms database downgrade
```

Step 6   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 the management service by using the **no cms enable** global configuration command.

```
(config)# no cms enable
```

Step 2   From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command.

```
CentralManager# cms database backup
```

Step 3   Install the pre-4.0.13 image by using the **copy ftp install** EXEC command.

Step 4   Reload the device.

Step 5   After the device reloads, enter the **cms database delete** EXEC command.

```
# cms database delete
```

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

Step 6   Initialize the CMS database tables by using the **cms database create** EXEC command.

```
# cms database create
```

Step 7   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 8   Enable the CMS service by using the **cms enable** global configuration command.

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

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 Wide Area Application Service (WAAS) Firmware download page (registered customers only). 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 in the file named L4_15427_FIRMWARE.zip.

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 when 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 4.0.15 and 4.0.17:

- Using Autoregistration with Port-Channel Interfaces
- WAFS Support of FAT32 File Servers

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.

Documentation Enhancements and Corrections

The following enhancements and corrections apply to the WAAS 4.0.13 documentation set:

- The following statement applies to the *Cisco Wide Area Application Services Configuration Guide*, Chapter 4, "Configuring Traffic Interception":

  For traffic from the WAN to the LAN where the destination MAC address of the next hop is a multicast MAC address, the Cisco WAE Inline Network Adapter does not optimize the traffic. The Cisco WAE Inline Network Adapter optimizes traffic only if the next hop MAC address is a unicast address.

- The following note clarifies this section in the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14, "Maintaining Your WAAS System," on page14-27:

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

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

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

- The WCCP GRE return egress method of WCCP interception allows you to place WAEs on the same VLAN or subnet as clients and servers. Repeating redirection is prevented by encapsulating the outgoing frames in the GRE frames. Cisco IOS routers handle these GRE frames as bypass frames and do not apply WCCP redirection. WAAS uses the router ID address as the destination for GRE frames. This technique makes it possible to support redundant routers and router load balancing and return frames back to the router from which they arrived. If you want to use this functionality with multiple routers connected to the WAAS network segment, you must ensure connectivity to the router ID address, for example, by configuring static routes.

  The router ID is the address of the first loopback interface or highest active physical interface. This address can be found in the output of the **show wccp routers** EXEC command.

- The **ip host** *hostname ip-address* global configuration command was added in version 4.0.13. This command adds an entry to the /etc/hosts file on the device, mapping the specified hostname to the specified IP address. A given hostname can be mapped only to a single IP address, while an IP address can have multiple hostnames mapped to it, each one through a separate issuance of this command.

  The command **no ip host** *hostname ip-address* removes the entry from the /etc/hosts file.

  The **ip host** command operates on devices in either the application-accelerator or central-manager device mode. This command has no default behavior.

  You can use the **show hosts** EXEC command to display the contents of the /etc/hosts file.

- The **external-ip** global configuration command is inadvertently documented in the *Cisco Wide Area Application Services Command Reference* but it is not part of the WAAS software.

- Any user account that has print admin privileges must also be assigned a domain, which defines the device groups or WAEs that are accessible by the user. All WAEs to which the user needs access should be members in the assigned domain.

  To assign a domain to a user account, from the WAAS Central Manager GUI, choose **System > AAA > Users**. Click the **Edit** icon next to the user account for which you want to assign domains. Click the **Assign** icon (blue cross mark) that appears next to the domain name that you want to assign to the selected user account. To save the changes, click **Submit**.

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

- The WAAS print server page log is stored in /local/local1/logs/cups_access_log. The cups_access_log file lists each page that is sent to a printer. Each line contains the following information:

  printer user job-id date-time page-number num-copies job-billing hostname

  Here is an example of a log entry:

  ```
  DeskJet root 2 [20/May/1999:19:21:05 +0000] 1 0 acme-123 localhost
  ```

  The field descriptions are as follows:

  - The *printer* field contains the name of the printer that printed the page. If you send a job to a printer class, this field will contain the name of the printer that was assigned the job.

  - The *user* field contains the name of the user (the IPP requesting-user-name attribute) that submitted this file for printing.

  - The *job-id* field contains the job number of the page being printed. Job numbers are reset to 1 whenever the CUPS server is started, so do not depend on this number being unique.

  - The *date-time* field contains the date and time when the page started printing. The format of this field is identical to the *date-time* field in the access_log file.

  - The *page-number* and *num-pages* fields contain the page number and number of copies being printed of that page. For printers that cannot produce copies on their own, the *num-pages* field will always be 1.

  - The *job-billing* field contains a copy of the job-billing attribute provided with the IPP create-job or print-job requests or "-" if none was provided.

  - The *hostname* field contains the name of the host (the IPP job-originating-host-name attribute) that originated the print job.

- When configuring print services, part of the process involves initializing each print driver on your WAAS print servers. After you complete the initialization step, perform the following additional steps before continuing:

  1. Run the print_diff utility for each print driver, to verify the driver installation on the Samba print server and to help you understand what printer features may not be supported. For details on this utility, see the Print_Diff Utility section in the document *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*.

  2. Run the print_fix utility for each print driver, to resolve any differences between the Samba and Windows print driver properties. For details on this utility, see the Print_Fix Utility section in the document *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*.

  3. Run the print_diff utility again for each print driver, to verify the driver properties after they were updated by the print_fix utility.

- The last sentence in the section "Calculating the TCP Buffers for High BDP Links" in Chapter 12, "Configuring Application Acceleration," in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:

  Once you calculate the size of the Max BDP, enter that value in the Send Buffer Size and Receive Buffer Size for the optimized connection on the Acceleration TCP Settings window.

- The description of the System.lcm.enable property in the section "Modifying the Default System Configuration Properties" in Chapter 9, "Configuring Other System Settings," in the *Cisco Wide Area Application Services Configuration Guide* should include the following information:

  If this property is set to false (disabled), configuration changes made on a local device will not be communicated to the Central Manager and configurations done in the Central Manager will overwrite local device configurations.

- Step 3 in the section "Installing Print Drivers on Individual WAAS Print Servers" in Chapter 13, "Configuring and Managing WAAS Print Services," in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:

  View the printers configured in the WAAS Print Server by opening the Printers folder.

- The note in Step 9e in the section "Creating an Application Policy" in Chapter 12, "Configuring Application Acceleration," in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:

> **Note** To specify a range of IP addresses, enter a wildcard subnet mask in either the destination or source IP Wildcard field.

Software Version 4.0.17 Open Caveats, and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.17:

- Software Version 4.0.17 Open Caveats
- Software Version 4.0.17 Resolved Caveats

Software Version 4.0.17 Open Caveats

The following open caveats apply to software version 4.0.17:

- **CSCsi66278**—When you access a fileshare on the DFS root of a NetApp filer, you see the following error message: NT_STATUS_NO_SUCH_FILE. Workaround: Remove the DFS root file server from the optimized servers configuration of WAAS. If the NetApp server is not defined in the optimized servers list but is auto-discovered, define the NetApp server as not exported in the Central Manager GUI.

- **CSCsi96571**—After a core WAE is taken down for maintenance and then brought back up, some of the edge WAEs do not reconnect to the core WAE on their own. Workaround: Reboot or restart edge services on those edge WAEs that failed to reconnect.

- **CSCsj69884**—When a WAE is configured using the Standby Interface feature, DHCP discovery requests continue to be generated even when a static IP address is configured. Workaround: None.

- **CSCsj75713**—When you add a new printer to the WAE-7341 or WAE-7371, you receive the following error message: server-error-service-unavailable. This message can be ignored. CUPS print services are not affected by this error. Workaround: None needed.

- **CSCsj99291**—A core dump occurs in the edge core_dir/ when you configure trusted domains and register the device to the Domain Controller using NTLM. Workaround: None

- **CSCsk13357**—Performance degradation due to DRE aggregation during NetApp SnapMirror optimization. Workaround: On WAN links slower than 45 Mbps, disable DRE aggregation by entering the **no dre agg enable** global configuration command. On links faster than 45 Mbps, disable DRE on the NetApp SnapMirror classifier (set the policy to TFO+LZ).

- **CSCsk36732**—The log message "RE Cache error: sub hash table is full" appears in the syslog. CPU spikes also occur during the issue. Workaround: Enter the **no dre agg enable** global configuration command and then clear the DRE cache.

- **CSCsk41815**—The /local/local1 (SYSFS) partition runs out of space when TFO transaction logging is enabled and there is a lot of traffic going through the box. TFO transaction logs are normally removed after two days, but if many connections occur in one day, they can fill up the disk. Workaround: Either disable the TFO transaction logging or remove the log files manually.

- **CSCsl03266**—Pressing the shutdown button on an NME-WAE module for less than one second does not cause a graceful shutdown per the device label. Workaround: Use a CLI command to gracefully shut down the device, as documented in the section "Shutting Down and Starting Up Cisco WAAS Network Modules" in *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.

- **CSCsl56564**—"Not in repository" message is shown for the printer drivers after switching the standby Central Manager to be 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 primary. Use the **windows-domain diagnostics tdb-list** command to list the tdb files. Use the **windows-domain diagnostics tdb-move** to move the tdb files.

- **CSCsl61189**—The system tries to authenticate a user using a secondary (local) login method when the primary authentication server is reachable. This occurs when the **Failover to next available authentication method** check box is checked and a tertiary or quaternary login method is specified. Workaround: Do not configure tertiary or quaternary login methods when the failover to next available authentication method option is enabled.

- **CSCsl64518**—When you make configuration changes from the Central Manager, they do not propagate to the edge WAEs after a rollback. This situation occurs when a rollback is performed on a Central Manager from 4.0.13 or higher to version 4.0.11 or earlier, and the WAEs are running version 4.0.13 or higher (a rollback to version 4.0.13 or higher works as expected). Workaround: None.

- **CSCsl70973**—A previously deleted classifier is getting pushed out from the Central Manager to some WAE devices and overwriting the AllDevicesGroup classifiers. Workaround: Perform the following steps:

  a. Remove the policies that are configured in the affected device by entering the **policy-engine config remove-all** global configuration command.

  b. After waiting two times the data feed poll rate (wait 10 minutes, by default), apply the AllDevicesGroup settings to the device by using one of the following methods:

  – Choose **AllDevicesGroup** in the drop-down list at the top of the Policy Definitions page (**Devices > Devices > Acceleration > Policy Definitions**) for each individual device and submit the page. (Do this step for all devices.)

  – Force the AllDevicesGroup device group settings to all devices by clicking the **Force Settings on all Devices in a Group** icon in the device group Policy Definitions page (**Devices > Device Groups > AllDevicesGroup > Acceleration > Policies > Definitions**). (Do this step only for devices that are affected.)

- **CSCsl76621**—The Central Manager GUI does not accept an inline interface's secondary IP address as the default gateway in the IP routes page if the inline interface's secondary IP address is on a different subnet than the destination address. This occurs when an inline interface is configured with both a primary IP address for data traffic and a secondary IP address for management traffic. Workaround: Configure the static route from the CLI by using the **ip route** global configuration command.

- **CSCsl80635**—On the WAE-674, the CIFS cache storage limit per specifications is not enforced. Workaround: When using the preposition feature, ensure that the total prepositioned data size does not exceed the CIFS cache size specifications. The system may reclaim storage capacity beyond the specifications without notice; the oldest content is removed first.

- **CSCsm18475**—The PXE/Altiris boot fails anytime the CIFS service is enabled because the directory bit is set for the batch file the client is trying to read. This occurs when there is a DOS client and a CIFS server that rejects LANMAN commands when working in DOS LM 1.2. Workaround: The workaround requires manual modification of internal configuration files. Please contact Cisco TAC/escalation for availability.

- **CSCsm42330**—After upgrading from software version 4.0.15, when the rescue CD is run to bring up the WAE-674, the swap disk partition size is only 3 GB. The size should be or 8 GB. The size of the swap partition is displayed by the CLI command **show memory**. Workaround: Execute the CLI command **disk delete-partitions** and then reload the WAE-674 device using **reload**. Note that this will delete all content on the disk.

- **CSCsm52918**—TFO accelerated connections fail to shutdown on a WAE device. This can occur when a pair of WAEs have TCP keepalives disabled. If a client or server resets a connection without a clean shutdown, a singular TCP RST packet is sent between the edge and core WAE devices. If that RST packet is lost or dropped because of network congestion, the lack of TCP keepalives prevents the intended WAE device from learning that the connection has been shutdown. The affected WAE will fail to reset the connection which may in turn be seen to persist indefinitely. Workaround: Ensure that TCP keepalives are enabled with he CLI command **tfo tcp keepalive**. This is the default setting for this configuration parameter. An administrator has to explicitly disable TFO TCP keepalives on the WAE device for this scenario to occur.

- **CSCsm55511**—The JVM process hangs for several seconds and fails to update its state in the policy engine. The following messages are recorded in syslog.txt:

```
Sysmon: %WAAS-SYSMON-: Fault detected: CIFS
Sysmon: %WAAS-SYSMON-: Fault cleared: CIFS
```

The following message is recorded in rx.internal.log:

```
:20:02,434  WARN (actona.util.policy.PolicyEngineNative:266) PolicyEngine keep alive
thread -  Failed to send KeepAlive err=:20:02,435  WARN
(actona.util.policy.PolicyEngineNative:272) PolicyEngine keep alive thread -
Time-out. Last call was [4836] ms ago, method call took 1ms, thread_prio=10
```

This issue does not affect existing CIFS connections. Only new CIFS connections established before the next keep-alive message are passed through (not optimized by CIFS). Workaround: None.

- **CSCsm89774**—After a client or server closes connections, a small subset of TCP connections fail to shutdown on a WAE device. This occurs when the WAE at one end of the connection is running software version 4.0.17 and the WAE at the other end is running version 4.0.15 or earlier. Workaround: None.

- **CSCsm50810**—Occasionally, the WAE-612-K9 may reboot automatically or enter KDB mode and hang when you perform a hard drive hot replacement using the following procedure:

    a. Enter the **disk disk-name disk00 shutdown** command.

    b. Remove one hard drive and insert a a new drive onto disk00.

    After performing the above hard drive replacement procedure with any set of supported Cisco hard drives of the same capacity (regardless of RPM speed) for the WAE-612, in some instances the WAE-612-K9 may reboot automatically or enter KDB mode and hang.

    Workarounds: Perform one of the following:

    – Upgrade to WAAS version 4.0.19 or later, in which the problem is fixed, before performing the hot swap procedure.

    – Perform a cold-swap procedure by first powering down the WAE-612 before swapping the drives.

    – If you do not upgrade to WAAS version 4.0.19 or later and the device hangs, power cycle the WAE-612-K9.

Note See "Cisco WAE-612 Hard Disk Drive Replacement Notification" for the notice that applies to the WAE-612 and all WAAS versions that support the hot-swap replacement of drives while the appliance is running.

Software Version 4.0.17 Resolved Caveats

The following caveats were resolved in software version 4.0.17:

- **CSCsl75349**—When the egress method is WCCP negotiated-return and the WAE is under a heavy CIFS traffic load (such as from a CIFS port scanner), a kernel crash occurs and core files are created.

- **CSCsm03286**—The network cannot establish a TCP connection through the WAE inline module when two subnets are configured on the same interface (router-on-a-stick topology). This occurs if the client and server exist in the same L2 environment but have different IP subnets and use the same router interface (configured with primary and secondary addresses).

- **CSCsm11550**—The WAE inline module intermittently loops SYN packets from WAN side. Because of network congestion, the SYN-ACK never reaches the client.

- **CSCsm22514**—Optimized TCP connections appear "stuck" in the WAE after the connection has been closed by the client and server. The symptoms for this issue include the following:
  - The optimized connection only appears in the client-side WAE.
  - The read and write states for the client-side original connection are both "Close".
  - The read state for the client-side optimized connection is "Read Shutdown".
  - The write state for the client-side optimized connection is "D. Write Wait".
  - The optimized connection read and work buffers contain data, usually 5 to 10 bytes.

- **CSCsm46924**—Flows persisted on the WAE even though there were no TCP keepalives on the client or server.

- **CSCsm51361**—Stale TCP connections on a WAAS device appear to be active and optimized, putting the WAAS in an overload state. Subsequent connections are forced into Passthrough mode. The connections are truly no longer active; the output of the CLI command **show tfo connection** displays:

```
Current Read State: Close Close
Previous Read State: Read Shutdown Read Shutdown
Current Write State: Close Close
Previous Write State: Write Shutdown Write Shutdown
```

- **CSCsm54004**—The WAE shows CPU usage spikes and performance appears to be affected. The tcpproxy appears to be using most of the CPU resources for a period of time.

Software Version 4.0.15 Open Caveats, Resolved Caveats, and Command Changes

The following sections contain the open caveats, resolved caveats, and command changes in software version 4.0.15:

- Software Version 4.0.15 Open Caveats
- Software Version 4.0.15 Resolved Caveats
- Software Version 4.0.15 New and Changed Commands

Software Version 4.0.15 Open Caveats

The following open caveats apply to software version 4.0.15:

- **CSCsi66278**—When you access a fileshare on the DFS root of a NetApp filer, you see the following error message: NT_STATUS_NO_SUCH_FILE. Workaround: Remove the DFS root file server from the optimized servers configuration of WAAS. If the NetApp server is not defined in the optimized servers list but is auto-discovered, define the NetApp server as not exported in the Central Manager GUI.

- **CSCsi96571**—After a core WAE is taken down for maintenance and then brought back up, some of the edge WAEs do not reconnect to the core WAE on their own. Workaround: Reboot or restart edge services on those edge WAEs that failed to reconnect.

- **CSCsj69884**—When a WAE is configured using the Standby Interface feature, DHCP discovery requests continue to be generated even when a static IP address is configured. Workaround: None.

- **CSCsj75713**—When you add a new printer to the WAE-7341 or WAE-7371, you receive the following error message: server-error-service-unavailable. This message can be ignored. CUPS print services are not affected by this error. Workaround: None needed.

- **CSCsj99291**—A core dump occurs in the edge core_dir/ when you configure trusted domains and register the device to the Domain Controller using NTLM. Workaround: None

- **CSCsk13357**—Performance degradation due to DRE aggregation during NetApp SnapMirror optimization. Workaround: On WAN links slower than 45 Mbps, disable DRE aggregation by entering the **no dre agg enable** global configuration command. On links faster than 45 Mbps, disable DRE on the NetApp SnapMirror classifier (set the policy to TFO+LZ).

- **CSCsk36732**—The log message "RE Cache error: sub hash table is full" appears in the syslog. CPU spikes also occur during the issue. Workaround: Enter the **no dre agg enable** global configuration command and then clear the DRE cache.

- **CSCsk41815**—The /local/local1 (SYSFS) partition runs out of space when TFO transaction logging is enabled and there is a lot of traffic going through the box. TFO transaction logs are normally removed after two days, but if many connections occur in one day, they can fill up the disk. Workaround: Either disable the TFO transaction logging or remove the log files manually.

- **CSCsl03266**—Pressing the shutdown button on an NME-WAE module for less than one second does not cause a graceful shutdown per the device label. Workaround: Use a CLI command to gracefully shut down the device, as documented in the section "Shutting Down and Starting Up Cisco WAAS Network Modules" in *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.

- **CSCsl56564**—"Not in repository" message is shown for the printer drivers after switching the standby Central Manager to be 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 primary. Use the **windows-domain diagnostics tdb-list** command to list the tdb files. Use the **windows-domain diagnostics tdb-move** to move the tdb files.

- **CSCsl61189**—The system tries to authenticate a user using a secondary (local) login method when the primary authentication server is reachable. This occurs when the **Failover to next available authentication method** check box is checked and a tertiary or quaternary login method is specified. Workaround: Do not configure tertiary or quaternary login methods when the failover to next available authentication method option is enabled.

- **CSCsl64518**—When you make configuration changes from the Central Manager, they do not propagate to the edge WAEs after a rollback. This situation occurs when a rollback is performed on a Central Manager from 4.0.13 or higher to version 4.0.11 or earlier, and the WAEs are running version 4.0.13 or higher (a rollback to version 4.0.13 or higher works as expected). Workaround: None.

- **CSCsl70973**—A previously deleted classifier is getting pushed out from the Central Manager to some WAE devices and overwriting the AllDevicesGroup classifiers. Workaround: Perform the following steps:

  a. Remove the policies that are configured in the affected device by entering the **policy-engine config remove-all** global configuration command.

    b. After waiting two times the data feed poll rate (wait 10 minutes, by default), apply the AllDevicesGroup settings to the device by using one of the following methods:

     – Choose **AllDevicesGroup** in the drop-down list at the top of the Policy Definitions page (**Devices > Devices > Acceleration > Policy Definitions**) for each individual device and submit the page. (Do this step for all devices.)

     – Force the AllDevicesGroup device group settings to all devices by clicking the **Force Settings on all Devices in a Group** icon in the device group Policy Definitions page (**Devices > Device Groups > AllDevicesGroup > Acceleration > Policies > Definitions**). (Do this step only for devices that are affected.)

- **CSCsl75349**—When the egress method is WCCP negotiated-return and the WAE is under a heavy CIFS traffic load (such as from a CIFS port scanner), a kernel crash occurs and core files are created.

   Workarounds:

    – Upgrade to software version 4.0.17 or later.

    – The source of the CIFS traffic may be a virus infected PC. Disinfect or disable the PC if that is the case.

    – Use ip-forwarding as the egress method, instead of WCCP negotiated-return.

    – Disable CIFS optimization.

- **CSCsl76621**—The Central Manager GUI does not accept an inline interface's secondary IP address as the default gateway in the IP routes page if the inline interface's secondary IP address is on a different subnet than the destination address. This occurs when an inline interface has both a primary IP address for data traffic and a secondary IP address for management traffic. Workaround: Configure the static route from the CLI by using the **ip route** global configuration command.

- **CSCsl80635**—On the WAE-674, the CIFS cache storage limit per specifications is not enforced. Workaround: When using the preposition feature, ensure that the total prepositioned data size does not exceed the CIFS cache size specifications. The system may reclaim storage capacity beyond the specifications without notice; the oldest content is removed first.

- **CSCsm03286**—The network cannot establish a TCP connection through the WAE inline module when two subnets are configured on the same interface (router-on-a-stick topology). This occurs if the client and server exist in the same L2 environment but have different IP subnets and use the same router interface (configured with primary and secondary addresses). Workaround: Upgrade to software version 4.0.17 or later.

- **CSCsm11550**—The WAE inline module intermittently loops SYN packets from WAN side. Because of network congestion, the SYN-ACK never reaches the client. Workaround: Upgrade to software version 4.0.17 or later.

- **CSCsm18475**—The PXE/Altiris boot fails anytime the CIFS service is enabled because the directory bit is set for the batch file the client is trying to read. This occurs when there is a DOS client and a CIFS server that rejects LANMAN commands when working in DOS LM 1.2. Workaround: The workaround requires manual modification of internal configuration files. Please contact Cisco TAC/escalation for availability.

- **CSCsm22514**—Optimized TCP connections appear "stuck" in the WAE after the connection has been closed by the client and server. The symptoms for this issue include the following:

    – The optimized connection only appears in the client-side WAE.

    – The read and write states for the client-side original connection are both "Close".

    – The read state for the client-side optimized connection is "Read Shutdown".

    – The write state for the client-side optimized connection is "D. Write Wait".

– The optimized connection read and work buffers contain data, usually 5 to 10 bytes.

Workarounds:

– Upgrade to software version 4.0.17 or later.

– Try restarting tcp proxy using the CLI command **service restart tcpproxy** when the problem is seen. If the problem persists then reboot the WAE.

- **CSCsm42330**—After the rescue CD is run to bring up the WAE-674, the swap disk partition size is only 3 GB. The size should be either 4 or 8 GB. The size of the swap partition is displayed by the CLI command show memory. Workaround: Execute the CLI command **disk delete-partitions** and then reload the WAE-674 device using **reload**. Note that this will delete all content on the disk.

- **CSCsm46924**—Flows persisted on the WAE even though there were no TCP keepalives on the client or server.

Workarounds:

– Upgrade to software version 4.0.17 or later.

– Try restarting tcp proxy using the CLI command **service restart tcpproxy** when the problem is seen. If the problem persists then reboot the WAE.

- **CSCsm51361**—Stale TCP connections on a WAAS device appear to be active and optimized, putting the WAAS in an overload state. Subsequent connections are forced into Passthrough mode. The connections are truly not active; the output of the CLI command **show tfo connection** displays:

```
Current Read State: Close Close
Previous Read State: Read Shutdown Read Shutdown
Current Write State: Close Close
Previous Write State: Write Shutdown Write Shutdown
```

This condition can occur when the system is upgraded from WAAS version 4.0.11 to 4.0.15 and the DRE cache is updated based on FIFO. The result is a deadlock situation that hangs the tcpproxy threads resulting in hung connections.

Workarounds:

– Upgrade to software version 4.0.17 or later.

– Try restarting tcp proxy using the CLI command **service restart tcpproxy** when the problem is seen. If the problem persists then reboot the WAE.

- **CSCsm52041**—The WAE stops processing flows going through TFO/DRE/LZ. If WCCP is removed, the flows bypass the WAE and operation is restored. Workaround: Try restarting tcp proxy using the CLI command **service restart tcpproxy**. If the problem persists then reboot the WAE.

- **CSCsm52918**—TFO accelerated connections fail to shutdown on a WAE device. This can occur when a pair of WAEs have TCP keepalives disabled. If a client or server resets a connection without a clean shutdown, a singular TCP RST packet is sent between the edge and core WAE devices. If that RST packet is lost or dropped because of network congestion, the lack of TCP keepalives prevents the intended WAE device from learning that the connection has been shutdown. The affected WAE will fail to reset the connection which may in turn be seen to persist indefinitely. Workaround: Ensure that TCP keepalives are enabled with he CLI command **tfo tcp keepalive**. This is the default setting for this configuration parameter. An administrator has to explicitly disable TFO TCP keepalives on the WAE device for this scenario to occur.

- **CSCsm54004**—The WAE shows CPU usage spikes and performance appears to be affected. The tcpproxy appears to be using most of the CPU resources. This happens during general operation when the logging file system is almost full, or rarely in slow or lossy WAN network scenarios. Workaround: Upgrade to software version 4.0.17 or later.

- **CSCsm55511**—The JVM process hangs for several seconds and fails to update its state in the policy engine. The following messages are recorded in syslog.txt:

```
Sysmon: %WAAS-SYSMON-: Fault detected: CIFS
Sysmon: %WAAS-SYSMON-: Fault cleared: CIFS
```

The following message is recorded in rx.internal.log:

```
:20:02,434  WARN (actona.util.policy.PolicyEngineNative:266) PolicyEngine keep alive
thread -  Failed to send KeepAlive err=:20:02,435  WARN
(actona.util.policy.PolicyEngineNative:272) PolicyEngine keep alive thread -
Time-out. Last call was [4836] ms ago, method call took 1ms, thread_prio=10
```

This issue does not affect existing CIFS connections. Only new CIFS connections established before the next keep-alive message are passed through (not optimized by CIFS). Workaround: None.

- **CSCsm89774**—After a client or server closes connections, a small subset of TCP connections fail to shutdown on a WAE device. This occurs when the WAE at one end of the connection is running software version 4.0.17 and the WAE at the other end is running version 4.0.15 or earlier. Workaround: None.

- **CSCsm50810**—Occasionally, WAE-612-K9 may reboot automatically or enter KDB mode and hang when you perform a 15K RPM hard drive hot replacement by following one of the following procedures:

Procedure #1: Replace 10K hard drive with 15K hard drive in a WAE-612-K9 with two working 300k 10k rpm drives

  a. Enter the **disk disk-name disk00 shutdown** command.

  b. Remove the 10k disk and insert a 300G 15K drive onto disk00.

Procedure #2: Replace 15K hard drive with 10K hard drive in a WAE-612-K9 with two 300k 15k rpm drives

  a. Enter the **disk disk-name disk00 shutdown** command.

  b. Remove the 15k disk and insert a 300G 10K drive onto disk00.

After performing one of the above hard drive replacement procedures, in some instances the WAE-612-K9 may reboot automatically or enter KDB mode and become unresponsive.

Workaround: Power cycle the WAE-612-K9.

Note See "Cisco WAE-612 Hard Disk Drive Replacement Notification" for the notice that applies to the WAE-612 and all WAAS versions that support the hot-swap replacement of drives while the appliance is running.

Software Version 4.0.15 Resolved Caveats

The following caveats were resolved in software version 4.0.15:

- **CSCsf02614**—WAFS misses keepalive (PE error code 246).

- **CSCsh93105**—When both edge and core WAEs are configured to use WCCP L2 redirect and IP forwarding as the egress method (IP forwarding is the default), they continue to use an MSS value of 1432 even though it is possible to use 1460. Changing the MSS value to 1460 by using the **tfo tcp optimized-mss 1460** or **tfo tcp original-mss 1460** global configuration commands does not work, and the WAEs continue to use an MSS value of 1432.

- **CSCsi10702**—When you replace the Central Manager either by performing a backup and restore of the Central Manager database or by adding a standby Central Manager, the print drivers are not backed up or passed to the standby Central Manager.

- **CSCsi32565**—Need a way to disable reverse DNS on the core WAE.

- **CSCsi33808**—After a WAAS Central Manager database backup is restored, a WAE device reports that the current WAAS Central Manager activation timestamp is older than expected, so configuration changes are not propagated to the WAE device.

- **CSCsi98147**—Print admin unable to delete print job.

- **CSCsj43783**—WAFS CIFS statistics pie chart is blank, even though an alias has been successfully configured, acceleration is occurring, and you are able to browse shares using the alias created for the configured server.

- **CSCsj80333**—When you transfer files to a CIFS share with a MAC client running MAC OS version 10.4.10, all of the MAC clients receive a "Finder Error-36" when they attempt to push the file.

- **CSCsj93996** and **CSCsk72549**—New Zealand daylight savings time update needs to be implemented.

- **CSCsj99810**—Prepositioning tasks end with an error message when the first root directory defined does not exist on the file server. The other directories are not prepositioned either.

- **CSCsk04140**—Traffic is dropped when inline mode is used in conjunction with non-multihop BGP as the BGP traffic will terminate at the WAE and will not reach its destination (that is, from switch to router).

- **CSCsk16004**—The traffic statistics report shows the wrong time stamp.

- **CSCsk18786**—Error log contains the following error after a reboot: %WAAS-CLI-3-170082: Verifier didn't respond. Need to re-register verifier. when setting cfg/gl/cache/wccp/service_data_base in data server (Error number: 64).

- **CSCsk22919**—A non-admin user is not able to see some charts of monitoring statistics; they see the error message "Insufficient privileges."

- **CSCsk23851**—DRE sees increasing and large latencies because DRE is not recognizing and handling an overload situation appropriately.

- **CSCsk24498**—The Last evicted resource access time value that is reported in the **WAFS Edge > Monitoring > Cache** page of the Device Manager GUI is incorrect.

- **CSCsk33567**—A remote Microsoft Access database query does not return the latest updated content.

- **CSCsk37824**—The WAAS Central Manager fails to save user preferences if there are too many WAEs registered to the CM. About 20 sets of user preferences can be saved. Each user can generate one set of user preferences for each registered WAE.

- **CSCsk47177**—Dual inline group use causes optimized connections to reset.

- **CSCsk62076**—When many clients access the same file using WAFS, this error results: Too many stuck requests. System will restart. Then the CIFS process restarts.

- **CSCsk66799**—Low throughput for more than 2000 connections between peers.

- **CSCsk71059**—File data is corrupted when using Linux CIFS VFS client.

- **CSCsk82726**—With WAAS 4.0.13 and the CIFS adapter active, when the client browses to a remote share folder, the folder appears empty.

- **CSCsk96255**—The CIFS cache serves a corrupted file after a specific and unique sequence of write requests followed by a read request.

- **CSCsl08795**—When the WAE is running a 16-bit application, the application is not able to see folders with a name longer than the standard 8.3 DOS format on a remote share through WAFS.

- **CSCsl15609**—Core file was generated after TCP proxy was restarted.

- **CSCsl25304**—The file server exported name that is sent to the edge device in non-transparent mode is incorrect and different from what the user sees in the Connectivity directive in the Central Manager GUI. This occurs when the file server name is entered as an IP address.

- **CSCsl31006**—Port channel 2 has been removed but the channel-group configuration inside the interface still prompts for both 1 and 2.

Software Version 4.0.15 New and Changed Commands

Table 4 lists the new commands and options that have been added in WAAS software version 4.0.15.

Table 4   CLI Commands Added in Version 4.0.15

Mode	Command and Syntax
EXEC	**test self-diagnostic** [**system**	**basic**	**connectivity**	**interfaces**	**tfo**	**wccp**	**inline**	**wafs**	**all**] For details, see the "test" section on page 28.
Interface configuration	**encapsulation dot1Q** *VLAN* This command is available only for inlineGroup interfaces. For details, see the "Configuring an Inline Interface from the CLI" section on page 6.

Table 5 lists existing commands that have been modified in WAAS version 4.0.15.

Table 5   CLI Commands Modified in Version 4.0.15

Mode	Command and Syntax	Description
EXEC	**reload** [**in** *m*] [**cancel**]	The **reload** command is enhanced with the option to schedule a software reload in *m* minutes (*m* can be 1-10080 minutes). After issuing this command, you are asked to confirm the reload by typing "y" and then confirm WCCP shutdown by typing "y" again (if WCCP is active). You can use the **cancel** option to cancel a scheduled reload.
	setup	The **setup** command is enhanced to configure more device settings.
	show interface inlineGroup *slot/grpnumber*	The **show interface** command has been enhanced to show IP address information for inline interfaces.
Global configuration	**primary-interface inlineGroup** *slot/grpnumber*	The **primary-interface** command is enhanced to allow setting an inline interface as the primary interface.
Interface configuration	**ip address** *ip-address ip-subnet* [**secondary**]	The **ip** command is enhanced to support IP address configuration on inline interfaces.

Table 6 lists commands that have been removed in WAAS version 4.0.15.

Table 6   ***CLI Commands Removed in Version 4.0.15***

Mode	Command
EXEC	**clear statistics epm**
	debug epm
	show adapter epm
	show statistics epm
Global configuration	**adapter epm enable**
	policy-engine application map adaptor EPM
	This command was not removed, but it is now ignored.

test

To perform diagnostic tests and display the results, use the **test** command.

test self-diagnostic {[system | basic | connectivity | interfaces | tfo | wccp | inline | wafs] | all}

SyntaxDescription	system	(Optional) Checks device status, presence of core files, and alarms.
	basic	(Optional) Checks device network configuration.
	connectivity	(Optional) Checks if the external hosts required for device operation are reachable by sending ICMP ping packets.
	interfaces	(Optional) Checks operation of physical interfaces, including ports on the Cisco WAE Inline Network Adapter.
	tfo	(Optional) Checks the traffic optimization configuration settings and operation. (Applies only to application accelerator devices.)
	wccp	(Optional) Checks the WCCP configuration settings and operation. (Applies only to application accelerator devices.)
	inline	(Optional) Checks the inline group configuration settings and operation. (Applies only to application accelerator devices that have the Cisco WAE Inline Network Adapter installed.)
	wafs	(Optional) Checks the WAFS configuration settings and operation. (Applies only to application accelerator devices.)
	all	(Optional) Runs all of the diagnostic tests.

Command Modes   EXEC mode

Device Modes   application-accelerator

                       central-manager

Usage Guidelines   If you use the **test self-diagnostic** command with the **all** option, all applicable tests are performed. You can specify one or more test options to perform just those tests.

The last diagnostic test report is stored on the device in the following file: /core_dir/diagnostic_report.txt.

Examples   The following example shows how to perform the basic, connectivity, interfaces, and WCCP tests:

```
WAE# test self-diagnostic basic connectivity interfaces wccp
```

Table 7 describes the error messages that can be returned by the **test self-diagnostics** command.

Table 7   Error Codes Returned by the test self-diagnostics Command

Test	Error Code	Description
system	HAS_COREDUMP	Core files are present.
	HAS_ALARM	Critical or major alarms are pending.
basic	NO_PRIM_IFACE	The primary interface is not configured.
	NO_PRIM_ADDR	The primary interface has no IP address configured.
	NO_HOSTNAME	The hostname is not configured.
	NO_NAMESERVER	The name servers are not configured.
	NO_DOMAIN	The domain name is not configured.
	NO_DEFAULT_GW	The default gateway is not configured.
	NO_CM_ADDR	The WAAS Central Manager IP address is not configured.
	NO_NTP_CFG	The NTP server is not configured.
connectivity	UNREACHABLE	The default gateway, name servers, NTP servers, authentication servers (RADIUS, TACACS, or Windows domain), or WAAS Central Manager are unreachable.
	UNRESOLVABLE	The fully qualified domain name of the device cannot be resolved.
interfaces	IFACE_DOWN	The interface is in shutdown mode. If all interfaces are shut down, the test will fail.
	IFACE_BW	The interface is configured or negotiated to use 10-MB speed instead of a faster speed.
	IFACE_HD	The interface is configured or negotiated to use half duplex instead of full duplex.
	IFACE_ERRORS	The interface has packet errors on more than 1 percent of received or sent packets.
	IFACE_COLLISIONS	The interface has packet collisions on more than 1 percent of sent packets.
tfo	TFO_DISABLED	TFO is disabled.
	TFO_NO_DRE	DRE is disabled.
	TFO_NO_LZ	Compression is disabled.
	TFO_NOAOACCL	An application accelerator in the policy engine is not enabled to accelerate traffic.
wccp	NO_RTRCFG	WCCP is enabled but TCP promiscuous mode is not configured.
	NO_RTRLIST	The router list specified in WCCP configuration is not configured.
	UNREACHABLE	Configured WCCP routers are unreachable or other WAEs in the WCCP farm are unreachable.
	NO_WCCP_RTRS	The WAE and WCCP routers cannot communicate with each other.

Table 7   *Error Codes Returned by the test self-diagnostics Command (continued)*

Test	Error Code	Description
inline	INLINE_NO_INT	Traffic interception is not configured on the inlineGroup interface.
	INLINE_SHUTDOWN	The inlineGroup interface is shut down.
	INLINE_BYPASS	The inlineGroup interface is in bypass mode.
	INLINE_INTRCPT	The inlineGroup interface is not intercepting traffic.
wafs	NO_CONNECTIVITY	The edge and core WAEs do not have connectivity defined or the peer devices are unreachable.
	UNREACHABLE	The WAFS connectivity peers are unreachable.
	NO_WAFS_CONN	The WAFS transport is not established.

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.

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.