



# 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 version 4.0.19. 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](http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html).



**Note**

---

If you are running version 4.0.17 or earlier, we recommend that you upgrade to version 4.0.19 at your earliest convenience.

---

This release note contains the following sections:

- [WAAS Product Overview](#)
- [New Features](#)
- [Replication Accelerator Mode](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.19](#)
- [Upgrading from Version 4.0.x to 4.0.19](#)
- [Downgrading from Version 4.0.19 to a Previous Version](#)
- [Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade](#)
- [Cisco WAE-612 Hard Disk Drive Replacement Notification](#)
- [Operating Considerations](#)
- [Software Version 4.0.19 Open Caveats](#)



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Software Version 4.0.19 Resolved Caveats](#)
- [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 to 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 version 4.0.19 includes the following new features and changes:

- Replication accelerator device mode for data-center-to-data-center traffic optimization. For details see the [“Replication Accelerator Mode” section on page 3](#).
- Secure store mode that uses strong encryption algorithms and key management policies to protect certain data on the system, including encryption keys used by applications in the WAAS system, CIFS passwords, and user login passwords.
- Strong password mode allows you to select more stringent user password policies than the standard password mode. These policies include requiring more robust passwords, password aging, and more.
- Enhanced encryption key management provides for key retrieval from the standby Central Manager if the primary Central Manager fails. This function also provides stronger key generation algorithms and enhanced management features.
- Network Time Protocol (NTP) support for MD5 authentication.

## Replication Accelerator Mode

Replication accelerator mode is a new device mode for the WAAS accelerators. This mode is specifically optimized for replication applications that run between data centers. This mode is similar to application accelerator mode, but the WAE's optimization policies are tuned for data-center-to-data-center operations.

Configure your WAAS device to function as a replication accelerator using the **device mode replication-accelerator** global configuration command. All WAEs that participate in the replication must be in the replication accelerator mode.



### Note

WAEs must be in the same accelerator device mode to work together. For example, WAEs in the replication accelerator device mode will only work with other WAEs in the replication accelerator mode.

## 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, 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 version of WAAS.

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.



### Note

When you view the software version using the **show version EXEC** command, extra characters are displayed (“-development[adbu-relbld-1:/users1”). These characters do not affect operation of your WAAS system and you can ignore them. The correct version is displayed at the end of the string (“waas\_4.0.19-b14”).

## Upgrading from a Prerelease Version to Version 4.0.19

To upgrade from WAAS prerelease software to version 4.0.19, you must perform 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 4.0.19

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 4.0.19, 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 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 5](#). 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 4.0.19 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 6](#).
- When you upgrade WAAS devices to version 4.0.19, the EPM classification feature is disabled and removed from the CLI and Central Manager GUI. If you use a WAE with WAAS 4.0.19 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 4.0.19, 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 4.0.19, 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 6.) 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 5.](#))

## Managing Passwords after an Upgrade

WAAS software version 4.0.19 includes a strong password feature for improved security. Previous versions of the WAAS software do not have a strong password capability.



### Note

The following considerations apply to WAAS software version 4.0.19 with the strong password policy enabled. Strong passwords are disabled by default.

When you upgrade from a previous version to version 4.0.19 please note the following password considerations:

- Existing passwords from the older version will continue to work in version 4.0.19.
- 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 4.0.19 to a Previous Version

If you enable disk encryption in version 4.0.19 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 4.0.19, you must disable them before you downgrade WAAS to a previous version.

Locked-out user accounts will be reset upon downgrade.

This section contains the following topics:

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

## Downgrading to Version 4.0.17 or 4.0.13

To downgrade the WAAS Central Manager (not required for WAE devices) to version 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.
- 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 4.0.13 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-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 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 4.0.19:

- [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.

## Software Version 4.0.19 Open Caveats

The following open caveats apply to software version 4.0.19:

- **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.

- **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.
- **CSCsk36732**—The log message “RE Cache error: sub hash table is full” appears in the syslog and CPU spikes also occur. 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 a lot of traffic going through the WAE device. 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.
- **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.
- **CSCsl61189**—The system tries to authenticate a user using a secondary (local) login method when the primary authentication server is reachable. This situation 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.
- **CSCso03782**—When ACLs are applied to the Gigabit Ethernet interface, they are also applied to the inline interfaces. Workaround: Do not apply ACLs to the Gigabit Ethernet interface.
- **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.
- **CSCso35104**—When a RAID-5 hard disk fails in an WAE-7341, WAE-7371, or WAE-674, the SNMP trap is not generated. A disk failure alarm is generated but the corresponding “ciscoContentEngineDiskFailed” trap is not generated by SNMP. Workaround: None.
- **CSCso47539**—When you enter the **show alarms** CLI command, WAAS indicates that the node health manager was restarted and that the WAE should be restarted. However, there is no indication in the syslog that the node health manager was restarted. The following message is displayed:
 

```
NOTE: The Node Health Manager was restarted and Alarm information
      may be inconsistent; however all other Device functionality
      should be unaffected.
      This device should be reloaded at the earliest convenience.
```

 Workaround: None.
- **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.

- **CSCsq02964**—If a WAAS device is downgraded from version 4.0.19 to a previous release, and then upgraded back to version 4.0.19, the device mode changes. For example, the device mode may change from application accelerator to replication accelerator. Workaround: Disable the WAAS Centralized Management System (CMS) on the device being downgraded and upgraded.
- **CSCsq17009**—When you configure a custom time zone and summertime (daylight savings time) setting, the Edge services on the WAE restart every 5 minutes. As a result, CIFS connections are disrupted. Workaround: Use a predefined time zone setting.
- **CSCsq24325**—When secure store is enabled on the Central Manager and you press Enter at the password prompt, the following error message is displayed:  
“java.lang.ArrayIndexOutOfBoundsException: 1”. This situation occurs when you reboot the Central Manager, or when you use the **cms secure-store open** CLI command. Workaround: Type a valid password before pressing Enter.
- **CSCsq24705**—If you type an incorrect password twice and then type the correct password at the third prompt, the Central Manager displays the following message: “Attempt to enter pass-phrase failed, continue device boot without opening secure-store?(y/n):” This situation occurs while the Central Manager is booting and secure store is enabled. Workaround: Type the correct password again and the Central Manager will continue booting correctly.
- **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.
- **CSCsq33268**—When secure store is already enabled (open) on the standby Central Manager and you open it again using the Central Manager GUI, the standby Central Manager prompts you for the password instead of reporting that secure store is already open. Workaround: Type the password again, the standby Central Manager displays the correct message, “secure-store is already open.”
- **CSCsq43732**—The network analysis tool Tethereal crashes while attempting to capture a packet from the WAE device. This situation does not affect WAAS system operation. Workaround: None.
- **CSCsq46326**—The mouse movement is slow when a user views directory listings on a CIFS-accelerated file server. Workaround: None.
- **CSCsq48302**—The WAE-512 device hangs during a reboot from a recovery CD if the hard drive installed in Disk01 is defective. Workaround: Replace the defective hard drive.
- **CSCsq50614**—When secure store is enabled and you use the **Change CMS Secure Store** function to generate a new encryption key for the WAE devices in a device group, the Force Device Group icon is displayed on the Central Manager GUI. Workaround: Ignore the Force Device Group icon, the secure store feature is working properly, and Central Manager will correctly show that secure store is open for all WAE devices in the device group. If you want to apply a secure store change or clear operation, perform one of the following procedures:

To apply a secure store change operation, do the following:

- 
- Step 1** Wait until the Central Manager and WAE have communicated with each other (one data feed poll cycle; by default this is 300 seconds).
- Step 2** Click the Force Device Group icon again.
- The secure store change operation is applied on all WAE devices in the selected device group. The Force Device Group icon will reappear after one data feed poll cycle.
- Step 3** Ignore the Force Device Group icon. No further action is required.
- 

To apply a secure store clear operation, do the following:

- 
- Step 1** Wait until the Central Manager and WAE have communicated with each other (one data feed poll cycle; by default this is 300 seconds).
- Step 2** Select **Clear CMS Secure Store** check box.
- Step 3** Click **Submit**.
- Step 4** Click the Force Device Group icon.

The clear operation is applied on all WAE devices in the selected device group. The Force Device Group icon will not reappear after this operation.

---

- **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.

## Software Version 4.0.19 Resolved Caveats

The following caveats were resolved in software version 4.0.19:

- **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.
- **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.
- **CSCsk13357**—The system performance degrades due to DRE aggregation during NetApp SnapMirror optimization.
- **CSCsl03266**—Pressing the shutdown button on an NME-WAE module for less than one second does not cause a graceful shutdown as indicated on the device label.
- **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.
- **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 situation occurs when an inline interface is configured with both a primary IP address for data traffic and a secondary IP address for management traffic.
- **CSCsl80635**—On the WAE-674, the CIFS cache storage limit per specifications is not enforced.
- **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 situation occurs if the client and server exist in the same Layer 2 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 the WAN side. Because of network congestion, the SYN-ACK never reaches the client.
- **CSCsm18475**—The PXE/Altiris boot fails when you enable the CIFS service because the directory bit is set for the batch file that the client is trying to read. This situation occurs when there is a DOS client and a CIFS server that rejects LANMAN commands in DOS LM 1.2.
- **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.
- **CSCsm42330**—After you upgrade from software version 4.0.15, when you run the rescue CD to bring up the WAE-674, the swap disk partition size is only 3 GB. The size should be 8 GB. The size of the swap partition is displayed when you enter the CLI command **show memory**.
- **CSCsm46924**—Flows persist on the WAE even though there are no TCP keepalives on the client or server.
- **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 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.

**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.

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

```
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.
- **CSCsm52918**—TFO accelerated connections fail to shut down on a WAE device 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 shut down. The affected WAE fails to reset the connection which may be seen to persist indefinitely.
- **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 situation occurs when the logging file system is almost full or in slow or lossy WAN network scenarios.
- **CSCsm55511**—The JVM process hangs for several seconds and fails to update its state in the policy engine. The following messages are recorded in the syslog.txt:

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

The following message is recorded in the 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 situation does not affect existing CIFS connections. Only new CIFS connections that are established before the next keepalive message are passed through (not optimized by CIFS).

- **CSCsm67027**—Applications that are using the CIFS cache receive file errors, such as “incorrect end of file 0xFFFFFFFF”.
- **CSCsq09927**—The Edge WAE restarts during high CIFS load conditions, and you see the error message “Negative reference count While releasing SMB server session object” in the Rx.internal.log.

## 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.

---

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

