Release Note for Cisco Wide Area Application Services

November 18, 2008

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

Contents

This release note applies to Cisco Wide Area Application Services (WAAS) software version 4.0.11. For information on WAAS features and commands, refer to the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

This release note contains the following sections:

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

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)

Changed Default Behavior for EPM Classification

In WAAS 4.0.9, EndPoint Mapper (EPM) Classification (or EPM adaptor) is disabled by default in the WAE, but enabled by default in the Central Manager. Because of this discrepancy, EPM Classification that is disabled in version 4.0.7, becomes enabled after you upgrade to version 4.0.9 when the Central Manager sends database updates along with its default settings to the WAEs in the network.

In WAAS 4.0.11, we have corrected the default discrepancies between the WAEs and the Central Manager, and we have added a new line in the code to disable EPM Classification for the following scenarios:

- Newly manufactured WAAS 4.0.11 WAEs and Central Managers after running the startup script
- Central Managers and WAES after an upgrade to 4.0.11
- WAEs with EPM Classification enabled when registered to a 4.0.11 Central Manager
- Any WAAS 4.0.11 device upon which the **restore factory defaults** command is used

To enable EPM Classification in 4.0.11, you must explicitly enable it after you upgrade to 4.0.11.

To enable EPM Classification, follow these steps:

Step 1 From the Central Manager GUI, choose **Devices > Device Groups**.

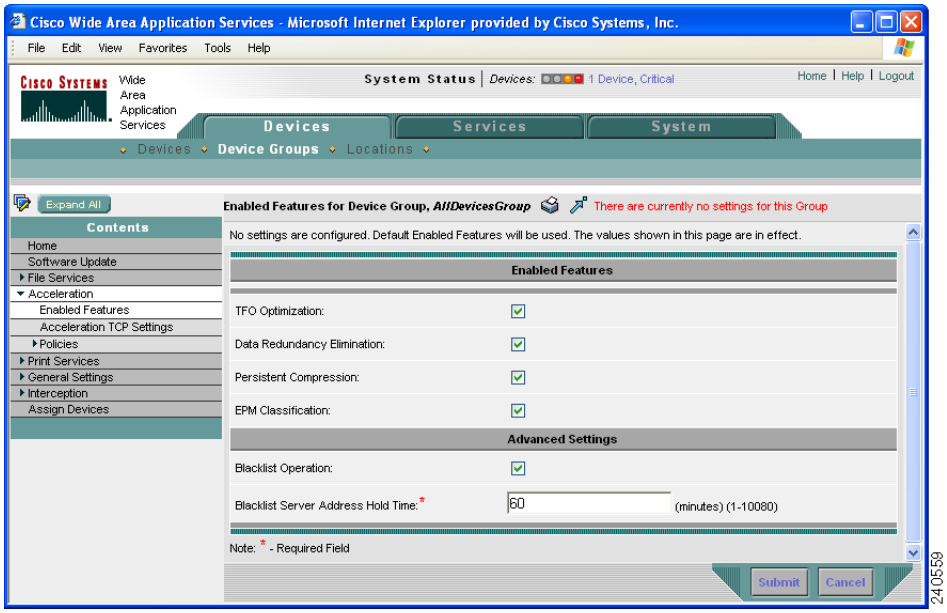
Step 2 Click the **Edit** icon next to the name of the device group for which you want to configure EPM Classification.

Step 3 In the Contents pane, choose **Acceleration > Enabled Features**. The Enabled Features for Device Group window appears.

Step 4 Check the EPM Classification check box, if not already checked.

Note When a device group does not have any active settings configured (see Figure 1), the check box for the EPM Classification option is checked by default. This setting is effective only when there is an active configuration.

Figure 1 Enabled Features for Device Group Screen Example (Showing No Settings)



Step 5 To activate the device group settings and enable EPM Classification, click **Submit**.

Step 6 To apply your device group settings to your devices, click the **Force Settings for All Devices in Group** icon in the taskbar. (See Figure 2.)

Figure 2 Force Settings on All Devices in Group Screen Example

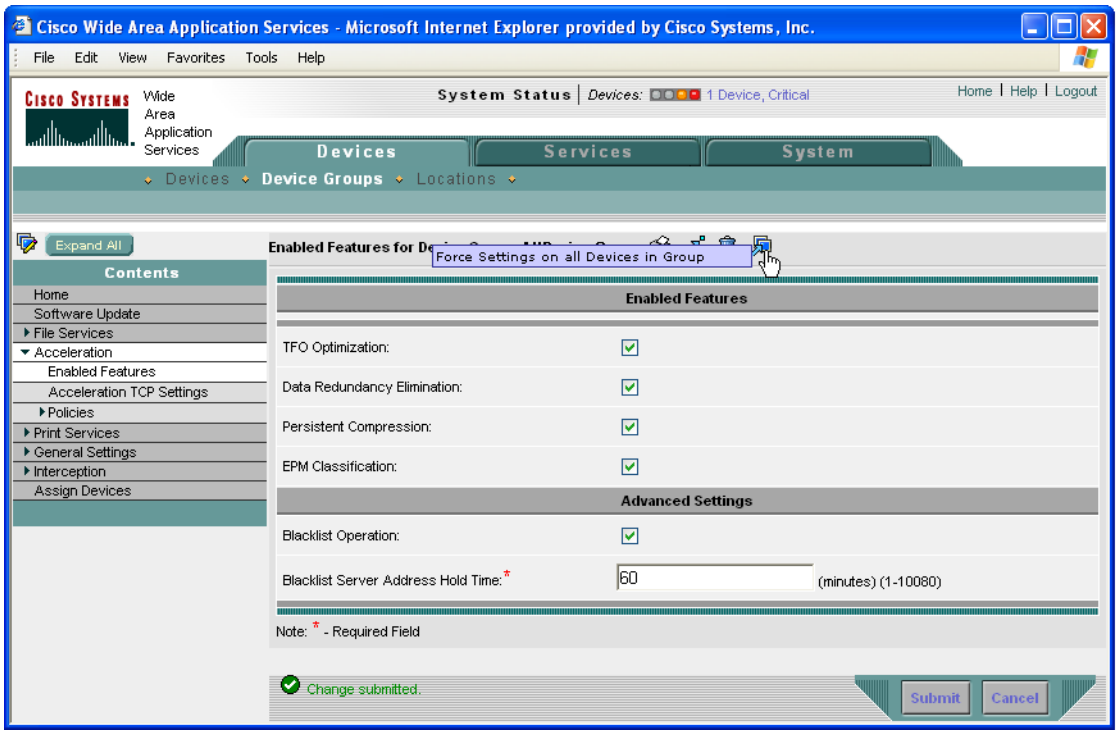


Figure 3 and Figure 4 demonstrate the changes that occur when you have a WAE with EPM Classification enabled and you upgrade the Central Manager to 4.0.11. Figure 3 shows a device that has EPM Classification enabled before the Central Manager is upgraded to 4.0.11. In this example, the device has current settings that have been applied from the device group named, AllDevicesGroup, which has EPM Classification enabled. This window is read-only.

Figure 3 Enabled Features for Device Screen Example (Showing Applied Settings from Device Group)

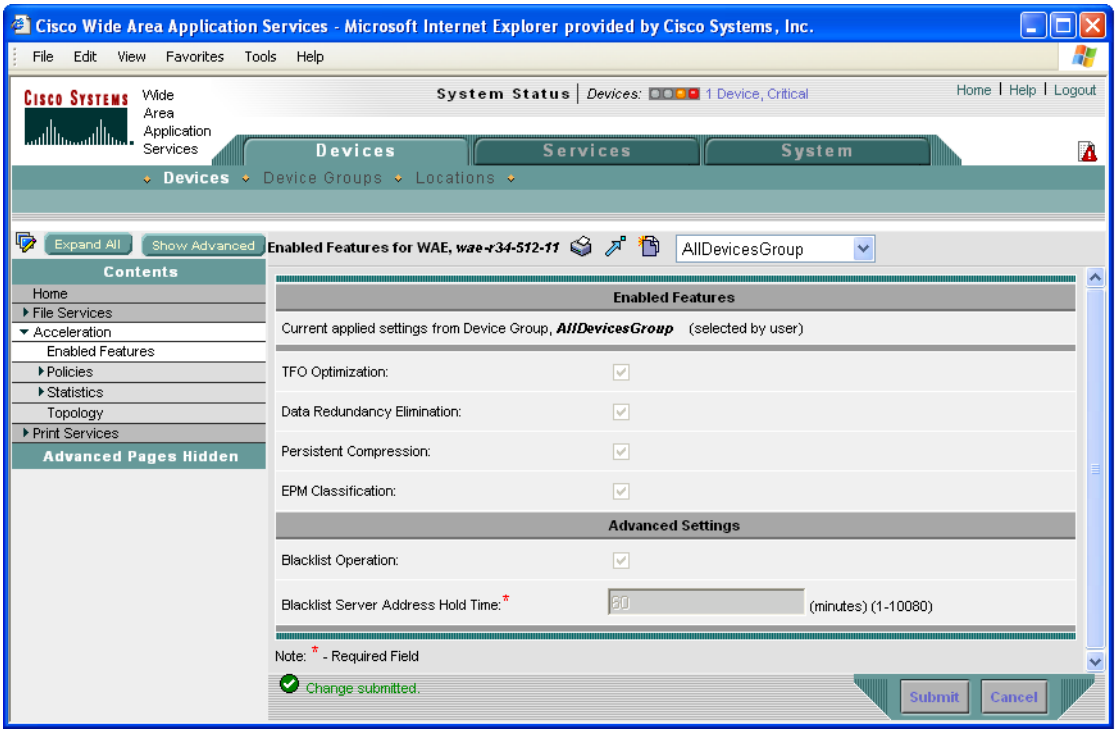
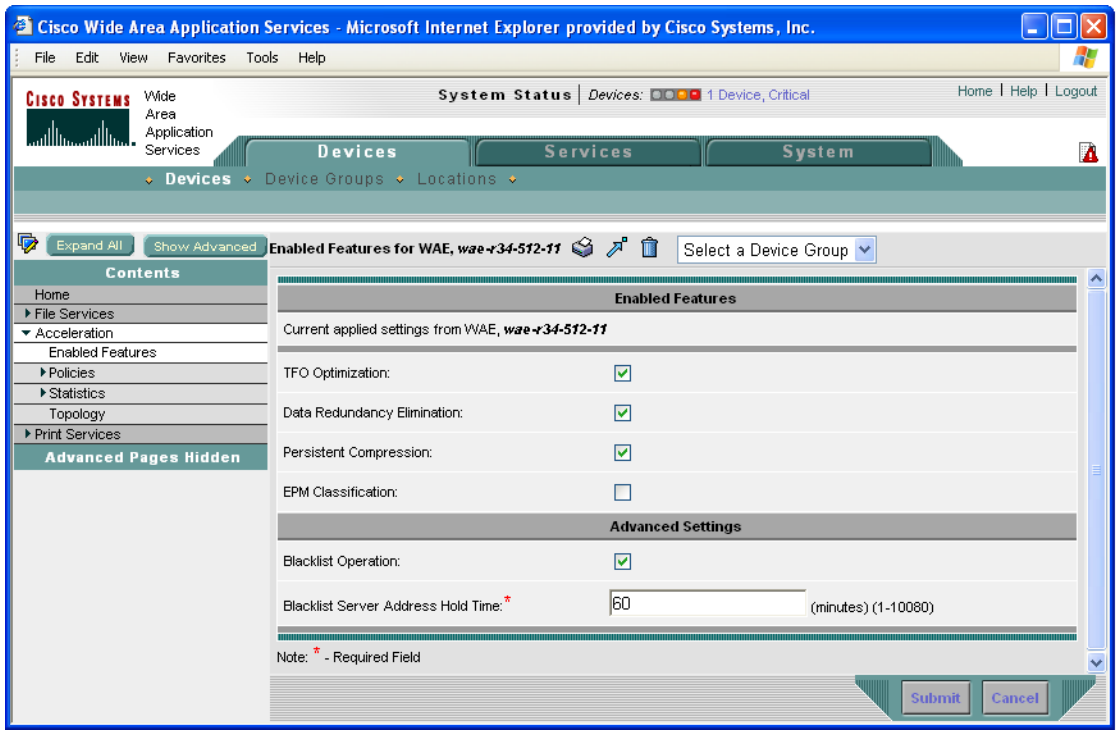


Figure 4 shows the same device window after the Central Manager has been upgraded to 4.0.11. After you upgrade the Central Manager to 4.0.11, the window enters device group override mode and becomes editable. The disabled EPM Classification device setting takes effect after an upgrade and overrides the enabled EPM Classification device group setting in the Central Manager GUI.

If you have the EPM Classification setting configured for a device group and you want to retain the device group settings for your devices after you upgrade your Central Manager to 4.0.11, click the **Force Settings for All Devices in Group** icon in the Enabled Features for Device Group window to force your device group settings on your devices. This icon only appears in the taskbar when the EPM Classification check box is checked and the configuration is active. (See Figure 2.)

Figure 4 Enabled Features for Device Screen Example (After Upgrading Central Manager to 4.0.11)



If you rollback from 4.0.11 to the previous version, you may disable EPM Classification during the rollback by using a downgrade script that has been designed for this purpose. To disable EPM Classification during rollback, follow these steps:

Step 1 From the Central Manager CLI, run the WAAS_Downgrade4_0_11_to_4_0_7 downgrade script by using the **cms database downgrade** command in EXEC mode, as shown in the following example:

```
CentralManager# cms database downgrade script WAAS_Downgrade4_0_11_to_4_0_7
```

This downgrade script disables EPM Classification.

Step 2 To check the previous version before you rollback the software, enter the **show version last** command in EXEC mode.

Step 3 From the WAE and the Central Manager CLI, enter the **restore rollback** command in EXEC mode.

```
WAE# restore rollback
CentralManager# restore rollback
```

Step 4 Verify that the rollback was successful by entering the **show version** command in EXEC mode.

Upgrading From WAFS to WAAS

Although WAFS to WAAS migration is supported, 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.

Upgrading from a Prerelease Version to Version 4.0.11

To upgrade from WAAS prerelease software to version 4.0.11, 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 4.0.11

This section contains the following topics:

Requirements and Guidelines

When you upgrade from version 4.0.x to version 4.0.11, 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, 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. See the "Running the WAAS Disk Check Tool" section on page 8.
- Upgrade the WAE devices first, and then upgrade the WAE Central Manager devices last.
- If you operate a network with devices that have different software versions, the WAAS Central Manager should be the lowest version.
- When you upgrade edge and core devices, 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 > Policies > 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.

- When you upgrade the Central Manager to version 4.0.11, the CIFS-non-wafs classifier is removed from edge and core devices automatically.

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 RAID Pairs Rebuild Successfully" section on page 9.) 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
Please disk_status.txt after reboot for result summary
umount: /state: device is busy
umount: /local/lPAM_unix[26162]: ### pam_unix: pam_sm_close_session (su) session closed
for user root
waitpid returns error: No child processes
No child alive.
```

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 RAID Pairs Rebuild Successfully

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

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 indicating 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," and "ext3_readdir: bad entry in directory."
- Other unusual behaviors related to disk operations or the inability to perform them.

If you encounter any of these symptoms, run the WAAS disk check tool to locate the problem. (For information about obtaining and using this tool, see the "Running the WAAS Disk Check Tool" section on page 8.)

Operating Considerations

This section includes operating considerations that apply to software version 4.0.11:

Using Full-Duplex Connections

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

WAAS Print Driver Support and Interoperability

WAAS WAE incorporates a Print Server based on the integration of open source Samba and CUPS technology. During the testing process, it has been determined that certain Print Drivers with complex features, such as sophisticated paper handling, may not be Point-and-Print compatible with WAAS. Most notably, Fiery Drivers incorporated into some Printer Manufacturer solutions are not compatible with Samba. Other Multi Function Printers (MFP) may also have limited functionality when working with Samba and are not supported by WAAS.

To determine if a Print Driver is compatible with WAAS, perform the Add Driver processes with a WAE using the Add Printer Wizard. Compare all the client Print features available after creating a print queue and compare it to a similar installation on a Microsoft Windows Print Server. If there are obvious feature inconsistencies, it is indicative of a Print Driver that cannot be used with WAAS Print Server for Point-and-Print. As a workaround, an installation on each client desktop from a CD or other source will be required.

When using the WAAS print services in a Windows XP Pro/Windows 2003 Server environment, you must register the WAE with Active Directory for the automatic printer driver download feature to operate correctly. This is due to a default computer policy for domain members that does not allow the host to download drivers from an unregistered device. A user will see a message similar to the following when encountering this issue: “A policy is in effect on your computer which prevents you from connecting to this print queue. Please contact your system administrator.”

The WAAS print solution does not offer authentication. Any user may access and send print jobs to the WAAS print server. Also, WAAS supports 32-bit drivers.

WAAS Print Services CUPS Log Files

Common Unix Printing System (CUPS) log files are rotated when the log file reaches the maximum size of 1 MB.

Ensuring Subnets are Reachable using Static or Dynamic Routing Protocols

The Cisco WAAS provides transparent optimizations, which preserves source and destination IP addresses and TCP header information. Because of this, the Cisco WAE device must be deployed on separate subnets than those existing on the LAN, both on the server side and on the client side. These standalone subnets, and the Cisco WAE devices attached to them, must be reachable from the Central Manager and other WAE devices. Ensure that these subnets are reachable using static or dynamic routing protocols. If the subnets are not reachable, critical WAE functions may be impaired, including file protocol optimizations, WAE management, central management, and management authentication.

Disabling the Automatic Machine Account Password Changes for the Edge WAE

In a WAAS network where a Windows domain controller is configured for authentication and Disconnected Mode is enabled on an edge WAE, the domain controller authenticates content requests in the event of a WAN failure. By default, Windows domain controllers enforce automatic machine account password changes as part of the authentication process. The machine account password for the edge WAE is automatically negotiated and changed between the edge WAE and the domain controller every seven days. However, if the authentication service is down, this process may not occur, and the machine account password for the edge WAE may expire.

To prevent this situation, we recommend that you disable automatic machine account password changes for the edge WAE. The procedure that follows describes how to disable automatic machine account password changes for Windows XP and Windows Server 2003 using Group Policy Editor. Refer to Microsoft's Help and Support page for details on how to disable automatic machine account password changes for other Windows operating systems.

To disable the automatic machine account password changes for the edge WAE using Group Policy Editor, follow these steps:

Step 1 On the domain controller, click **Start**, then choose **Run**.

Step 2 Enter **Gpedit** at the prompt, then click **OK**.

Step 3 Expand the Local Computer Policy, Windows Settings, Security Settings, Local Policies, Security Settings, Local Policies, Security Options.

Step 4 Configure the following setting: Domain Member: Disable machine account password changes (DisablePasswordChange).

Using PortFast with Inline Mode

When a WAE that has a Cisco WAE Inline Network Adapter installed enters bypass mode, the switch and router ports to which it is connected may have to reinitialize, and this may cause an interruption of several seconds in the traffic flow through the WAE.

If the WAE is deployed in a configuration where the creation of a loop is not possible (that is, if it is deployed in a standard fashion between a switch and a router), configure PortFast on the switch port to which the WAE is connected. PortFast allows the port to skip the first few stages of the Spanning Tree Algorithm (STA) and move more quickly into a packet forwarding mode.

Documentation Enhancements and Corrections

The following statement applies to the WAAS 4.0.11 document, *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.

Software Version 4.0.11 Open and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.11:

Software Version 4.0.11 Open Caveats

The following open caveats apply to software version 4.0.11:

- **CSCse71473**—After changing a local user's password when the old password is a prefix of the new password, the user's account encrypted password string is not changed. Additionally, only the first eight characters are used when setting a local account password.
- **CSCsg11506**—EndPoint Mapper (EPM)-based applications are unavailable in asymmetric routing scenarios. If the WAE receives packets going in one direction, but does not see packets returning from the other direction, the TFO handles this by establishing a pass-through. However, unlike the TFO, EPM always assumes that it will receive traffic going both directions and that the origin server is always up. EPM does not use autodiscovery. Instead, it terminates the 3-way handshake itself and establishes a new and separate spoofed TCP connection toward the server. Because of this behavior, if the server response bypasses the WAE (so that EPM does not intercept it), the client will receive a SYN+ACK for a TCP connection that it has already established and that has a different synchronization number. This situation causes the connection to be dropped. Workaround: Identify and resolve the cause of the asymmetric routing. If the cause of the asymmetric routing cannot be identified, or if a more immediate workaround is required, disable EPM. Acceleration will still be supported through the "Other" classifier. To disable EPM, enter the **no adapter epm enable** command in global configuration mode from the CLI, or edit the device in the Central Manager GUI by unchecking the EPM Classification check box from the Device **Acceleration > Enable Features** window.
- **CSCsg79439**—DRE chunk aggregation may cause severe performance degradation because the same file is transferred over the WAN repeatedly over time. When very large files (hundreds of megabytes to gigabytes in size) are transferred repeatedly over time, the disk cache becomes fragmented. Workaround: Clear the DRE cache.
- **CSCsh44391**—When using the Rsync, protocol a throughput drop is observed due to a large number of bytes bypassing the optimization module. This situation occurs when replicating a huge directory structure with hundreds of thousands of files using Rsync. Workaround: Increase the original TCP send/receive buffers to the maximum possible value (8 MB) as a partial work around. If the issue is still seen, break the transfer into multiple smaller transfers.

- **CSCsh51624**—The Central Manager **Acceleration > Enabled Features** (previously General Settings) page goes into override mode. This situation occurs when you uncheck the Blacklist Operation check box or change the Blacklist Server Address Hold Time on this page in a device group, assign the device group to a WAE, and then downgrade the Central Manager to a previous software version. Workaround: Click the **Force Settings for All Devices in Group** icon in the taskbar to apply your device group settings to your devices.
- **CSCsh72271**—The transfer time for large files and multiple files that contain the same data becomes very slow over time, even if you have disabled chunk aggregation (level0 chunks only). By clearing the DRE cache, transfer times are restored to expected levels.
- **CSCsh82935**—WAFS is locally failing write requests on files opened using an OpenPrintFile request. When users print from AutoCad, they get a STATUS_INVALID_HANDLE error message. The AutoCad printing feature does not use the Windows "Print" command. The CAD file is first copied to a billing system and the billing system transmits the file to a printer device in DOS. Workaround: None.
- **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. Workaround: Follow these steps:
  a. Ensure that the WAAS Central Manager has the correct time.
  b. From the WAAS Central Manager CLI, enter the following sequence of commands:

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

  c. From the WAAS Central Manager GUI, trigger full resynchronization of registered devices: choose **Devices > Device Groups > AllDevicesGroup** and click the **Force full database update** icon in the toolbar.
- **CSCsi90785**—An Edge WAE in inline mode with over 1500 static CIFS connections and 700 dynamic CIFS clients running entered KDB mode after two hours.

Software Version 4.0.11 Resolved Caveats

The following caveats were resolved in software version 4.0.11:

- **CSCsh69408**—The Central Manager sends updated configuration commands to a WAE for WCCP settings even when there is no change to the current running configuration. This situation occurs when a WCCP CLI change is made on a WAE that is managed by a Central Manager. This change is synchronized with the Central Manager, which then sends the change back to the WAE as CLI commands. The following commands are affected: **flow redirection**, **shutdown delay**, **slowstart**, **wccp router-list**, and **wccp version**.
- **CSCsh83544**—A login to the device manager GUI fails without any error message, regardless of the username or password used when a managed component (such as an edge or core appliance) contains a Size object with a negative value in its data.
- **CSCsh84963**—Preposition directive generates the wrong size number. This problem occurs for files larger than 2 GB that are already partially cached on demand.
- **CSCsi35007**—Files are retrieved from the target file server instead of from the WAFS preposition cache.

- **CSCsi44131**—A WAFS Edge WAE may incorrectly choose a Core WAE through CIFS auto-discovery when the Core WAE closest to the file server is heavily loaded and another Core WAE in a different location appears to be closer.
- **CSCsi44512**—WAFS logs a WARN message for every session that encounters SMB signed (or non-existing) servers, which overloads the message log.
- **CSCsi47369**—The **kernel kdb** command in global configuration mode returns to enabled after you disable it for a device group using Central Manager GUI.
- **CSCsi48683**—A timing-related deadlock issue causes the WAE to appear offline in the Central Manager GUI even though it is actually online and the **show cms info** command shows that it is online.
- **CSCsi49779**—EPM Classification that is disabled in version 4.0.7 becomes enabled after you upgrade to version 4.0.9. When you attempt to disable EPM classification from the Central Manager GUI (**Devices > Device Groups > Acceleration > Enabled Features > Enabled Features for Device Group,** *AllDevicesGroup*), the EPM Classification option is disabled only momentarily and then becomes re-enabled. To permanently disable the EPM adapter, you must disable it through the individual WAE CLI by entering the **no adapter epm enable** command in global configuration mode. (See the "Changed Default Behavior for EPM Classification" section on page 2.)
- **CSCsi58809**—The WAE may become deadlocked during CIFS auto-discovery when a client is infected with a virus that performs SYN scanning on port 445.
- **CSCsi66928**—A WAAS device that is functioning as a WAFS Edge may experience CPU usage nearing 100 percent and service disruptions. The message log fills with messages from the CIFS auto-discovery module, such as *host not found* or *timeout*.
- **CSCsi67248**—The WAE WAN-0 inline interface fails to reestablish a link to the Cisco 2821 router Gigabit Ethernet interface after the WAE loses power and reboots.
- **CSCsi67259**—When the WAE inline card WAN-0 cable that is connected to the Cisco 2821 router is disconnected and reconnected, the link between the WAN-0 interface and the router may fail to come up.
- **CSCsi81399**—Connectivity to the console of the default gateway is lost. This problem occurs when inline interception is enabled in the WAE and traffic is going through the inline module when the InlineGroup interface is shut down. This issue is seen only when the inline module is connected to a Catalyst 2950 switch.
- **CSCsj04543**—The network module (NM-WAE) may fail to join the Windows domain on reload. The root cause of this issue was found to be a misplaced statement that stops winbindd when the IP address is configured on a device. The problem applies to all hardware models, but shows up more frequently on the NM-WAE because of the way IP addresses are configured on the NM-WAE. The IP address on the NM-WAE is configured on the router; it is retrieved in an asynchronous manner during the reboot and might be configured after the startup configuration has been applied. On other appliances, IP addresses are configured as part of the startup configuration and before authentication-related CLIs in the startup configuration are configured. This difference apparently causes the issue to occur more frequently on NM-WAEs.

  It may take up to 15 minutes on the NM-WAE for Windows authentication to be fully functional after a reload.

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.