Release Note for Cisco Wide Area Application Services Software Version 4.1.5x

December 13, 2010

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

Contents

This release note applies to the following software versions for the Cisco Wide Area Application Services (WAAS) software:

- 4.1.5g
- 4.1.5f
- 4.1.5e
- 4.1.5d
- 4.1.5c
- 4.1.5b
- 4.1.5a
- 4.1.5

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 The WAAS Central Manager must be the highest version of all devices in your WAAS network. Upgrade the Central Manager first before any other devices.

This release note contains the following sections:

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

New and Changed Features

The following section contains the new and changed features in software version 4.1.5x:

Software Version 4.1.5d Functionality Changes

WAAS software version 4.1.5d includes the following funcationality changes:

- Troubleshooting Page Output Limit—The output for any command executed from the WAAS Central Manager GUI Troubleshooting Page (**My WAN > Manage Devices > Device > Show Commands**) will be limited to maximum of 30,000 lines, due to system resource constraints. If needed, you can use a filter to limit the output, or use the CLI on the device instead.

Software Version 4.1.5 New and Changed Features

WAAS software version 4.1.5 includes the following new features and changes:

- Web Application Filter—Web Application Filter is a security feature that protects the WAAS Central Manager GUI against Cross-Site Scripting (XSS) attacks. For more information, see the "Web Application Filter" section on page 3.

- Audit Log Entry—An entry is now added to the audit log when a user clears the audit logs.
- Privileged Level Required for the **cifs** Command—A user with privilege level 0 is no longer authorized to use the **cifs** command.
- Core Device Cipher List Priority—When SSL peering service is configured, the priority associated with a cipher list on a core device takes precedence over the priority associated with a cipher list on an edge device.
- Device Model in Device List—In the WAAS Central Manager GUI, the **My WAN > Manage Devices > Device** page now lists the device model.
- IP ACL Configurations Require Admin Privileges—Only a user with admin privileges is allowed to view, edit, or create IP ACL configurations in the Central Manager.
- SSL Device Certificate Configuration Moved—In the WAAS Central Manager GUI, the SSL Device Certificate Configuration has moved from the **Security > Peering Service > Peer Services** page to the **Security > SSL > Global Settings > SSL Global Settings** page.
- CPU Utilization Chart Support in the CPU Usage Report—In the WAAS Central Manager GUI, only the CPU Utilization chart is supported for the **Report > Manage Reports > CPU Usage** report page.
- Admin Access to Report Creator List—In the WAAS Central Manager GUI, for users with admin privileges, the creator of the report is shown on the **Report > Scheduled Reports > Scheduled Reports** page.
- Monitoring and Reporting Usability Enhancements—Monitoring and reporting tables have sort functionality, reports can be sent to multiple e-mail IDs, and the number of days can be specified on the **My WAN > Configure > System Properties** page to purge historical AO statistics.
- Monitoring and Reporting Area Chart Enhancements—Area comparison charts are more easily readable as line charts when more than three applications are selected. Note that this is only applicable to charts with user-selectable applications. In addition, all area charts with more than three applications selected and saved are converted to line charts after the upgrade.
- New Address Field for Email Notification—In the WAAS Central Manager GUI, an optional From Address field has been added to the **Configure > Monitoring > Email Notification > Configure Email Server Details** page.
- SNMP Trigger Wildcard Check Box Disabled—On the **Configure > Monitoring > SNMP > Trigger > Modifying SNMP Trigger** page, the Wildcard check box has been disabled.
- CLI commands—For CLI command changes, see the "Software Version 4.1.5 Command Changes" section on page 23.

Web Application Filter

Web Application Filter is a security feature that protects the WAAS Central Manager GUI against Cross-Site Scripting (XSS) attacks. XSS security issues can occur when an application sends data that originates from a user to a web browser without first validating or encoding the content, which can allow malicious scripting to be executed in the client browser, potentially compromising database integrity.

This security feature verifies that all application parameters sent from WAAS users are validated and/or encoded before populating any HTML pages.

This section contains the following topics:

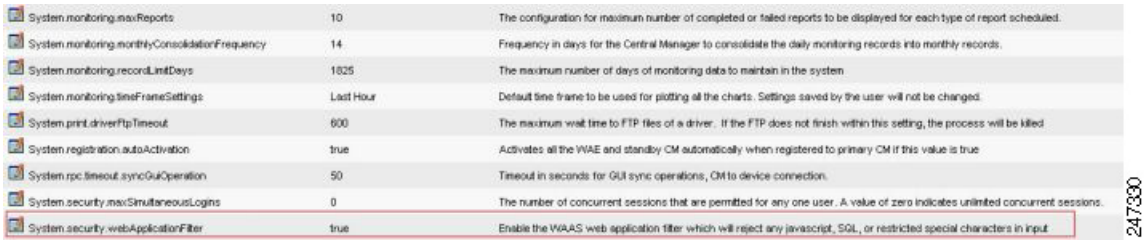
Enabling Web Application Filter

To enable the Web Application Filter, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **My WAN > System Property > Web Application Filter**. The System Property window appears. (See Figure 1.)

Note You cannot enable this feature using the CLI. This feature is disabled by default.

Figure 1 System Property List



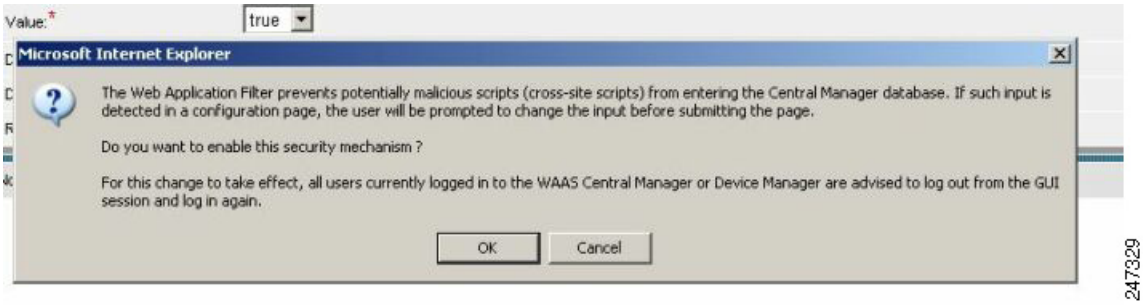
Step 2 Click the edit icon next to the system.security.webApplicationFilter entry.

The Modifying Config Property window appears.

Step 3 Choose **true** from the Value drop-down list to enable this feature.

A warning appears to advise Central or Device Manager users to log out and then back in after enabling this feature. (See Figure 2.)

Figure 2 Modifying Config Property



Step 4 Click **OK** and then **Submit**.

Step 5 Log out and then back in again.

Security Verification

The Web Application Filter feature verifies security using two methods, input verification and sanitization. Input validation validates all input data before accepting data. Sanitization prevents malicious configuration and scripts already present in the data from getting executed.

This section contains the following topics:

Input Validation

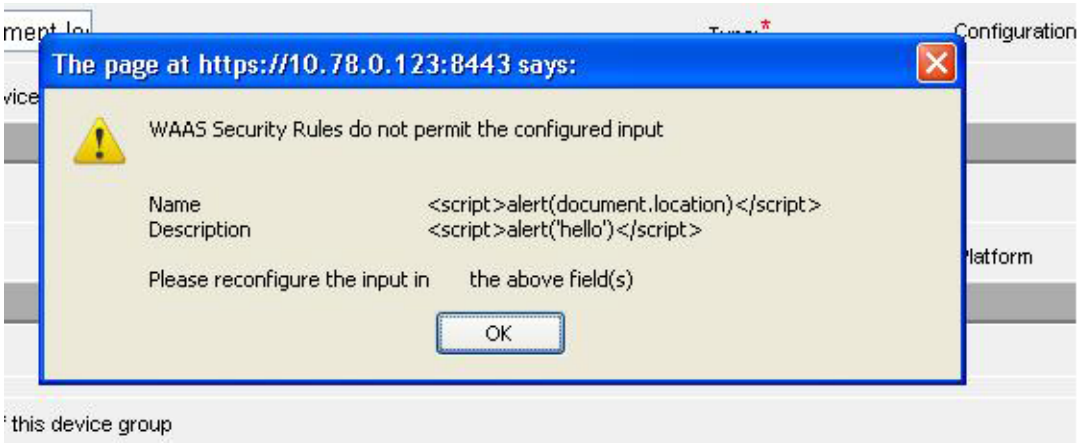
Input validation scans all data that is input to the Central/Device Manager database and is only configurable by the admin user.

Any input submitted using the Central Manager GUI that is suspicious of XSS is blocked. Blocked input results in a warning. (See Figure 3.)

Input data is checked against the following XSS filter rules:

- Input is rejected if it contains a semicolon (;)
- Input is rejected if it is enclosed in angle brackets (<>)
- Input is rejected if it can be indirectly used to generate the above tags (&#60, &#62, %3c, %3e)

Figure 3 Warning

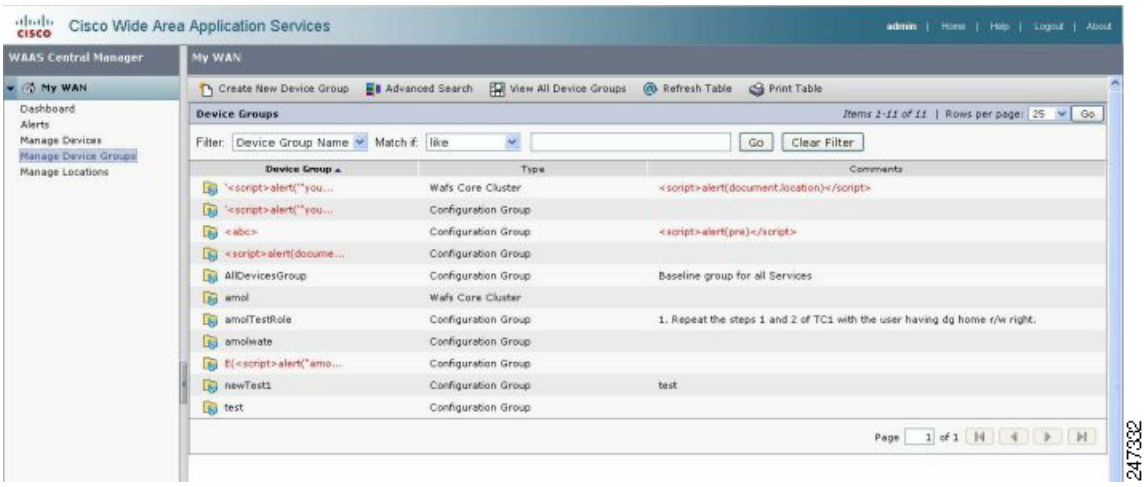


Sanitization

The sanitizer prevents malicious configuration and scripts from getting executed in the browser when there is an XSS attack on the database. Sanitization is not configurable by the user.

Configuration data coming from the Central Manager that is suspect for XSS is shown in red on the **My WAN > Manage Device Groups > Device Groups** page. (See Figure 4.)

Figure 4 XSS Configuration Data



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 released WAAS version; you cannot upgrade to a prerelease version of WAAS software.

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.
- After migrating from WAFS to WAAS, reenter the file server credentials from the WAAS Central Manager GUI.

Upgrading and Interoperability

This section contains the following topics:

Prepositioning Interoperability

Note When a Central Manager running version 4.1.5c or later is managing a WAE running a previous version (4.1.5b or earlier), you must use the Central Manager to create, modify, delete, and schedule preposition tasks.

This requirement is necessary because of preexisting behavior in WAE software versions 4.1.5b or earlier that causes schedule information, from a preposition task created on the WAE, to be discarded by the 4.1.5c or later Central Manager. Since the Central Manager cannot create a preposition task successfully without schedule information, the preposition task is automatically removed from the WAE.

In this case, although the Central Manager GUI indicates that the preposition schedule is NOW and the WAE has been assigned to the task, this information is misleading.

To recover from this scenario, for preposition tasks that were created on WAE software versions 4.1.5b or earlier to be successful with a Central Manager running version 4.1.5c or later, perform the following steps:

Step 1 Modify the schedule as required using the Central Manager GUI, even if you want the preposition schedule as NOW, and click Submit.

Step 2 Wait two data feed poll cycles for the configuration to synchronize between the Central manager and the WAE (default data feed poll cycle is 300 seconds).

The preposition task is then created on the WAE and the Central Manager, and the WAE is assigned to the preposition task with the required schedule changes.

In addition to GUI changes, any preposition changes made using the CLI on a WAE running version 4.1.5b or earlier are also discarded by the 4.1.5c or later Central Manager.

Therefore, you must also use the Central Manager to perform the following preposition CLI tasks:

- Create, modify, or delete schedule
- Delete pattern
- Modify or delete root-share

WCCP Interoperability

Central Managers running version 4.1.5x can manage WAEs running previous versions of 4.0.x and 4.1.x. However, it is recommended that all WAEs in a given WCCP farm be running the same version.

To upgrade the WAEs in your WCCP farm, follow these steps:

Step 1 You must disable WCCP redirection on the IOS router first. To remove the global WCCP configuration, use the following **no ip wccp** global configuration commands:

```
Router(config)# no ip wccp 61
Router(config)# no ip wccp 62
```

Step 2 For large WCCP farms (greater than 15), increase the buffer size on the IOS router to the maximum of 65535. This is necessary when WCCP is configured with mask assignment, using a mask with 6 or 7 bits. To set the buffer size to 65535, use the **buffers** global configuration command:

```
Router(config)# buffers huge size 65000
```

Step 3 Perform the WAAS software upgrade on all WAEs using the WAAS Central Manager GUI.

Step 4 Verify that all WAEs have been upgraded in the Devices pane of the WAAS Central Manager GUI. Choose **My WAN > Manage Devices** to view the software version of each WAE.

Step 5 Re-enable WCCP redirection on the IOS routers. To enable WCCP redirection, use the **ip wccp** global configuration commands:

```
Router(config)# ip wccp 61
Router(config)# ip wccp 62
```

Upgrading from a Prerelease Version to Version 4.1.5x

To upgrade from WAAS prerelease software to version 4.1.5x, 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 or 4.1.1x to 4.1.5x

This section contains the following topics:

Requirements and Guidelines

When you upgrade from version 4.0.x or 4.1.1x to version 4.1.5x, observe the following guidelines and requirements:

- Upgrading to the current 4.1.5x version is supported only from versions 4.0.19, 4.0.25, 4.1.1d, 4.1.3, 4.1.3b, and any previous 4.1.5x version. If you want to upgrade a WAAS device running a different version, first upgrade to 4.0.19, 4.0.25, 4.1.1d, 4.1.3, 4.1.3b, or any previous 4.1.5x version and then upgrade to the current 4.1.5x version.
- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version.
- If you operate a network with devices that have different software versions, the WAAS Central Manager must be the highest version.
- Upgrade the WAAS Central Manager devices first, and then upgrade the WAE devices. If you have a standby WAAS Central Manager, upgrade it first, before upgrading the primary WAAS Central Manager. After upgrading, restart any active browser connections to the WAAS Central Manager.

- Before upgrading a WAAS Central Manager to version 4.1.5x, make a database backup by using the **cms database backup** EXEC command. This command creates a backup file in /local1/. In case of any problem during the upgrade, you can restore the database backup that you made before upgrading by using the **cms database restore** *backup-file* EXEC command, where *backup-file* is the one created by the **backup** command.
- If you upgrade a WAAS Central Manager to 4.1.5x using the **Jobs > Software Update** page from a 4.0.x WAAS Central Manager, enter 4.1.5.4.7 in the Software Version field.
- After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If WAFS was enabled on the device before the upgrade, then the Enterprise license should be enabled. Configure any additional licenses (Video and Virtual-Blade) as needed by using the **license add** EXEC command. For more information on licenses, see the "Managing Software Licenses" section on page 9-3 in the *Cisco Wide Area Application Services Configuration Guide*.
- After upgrading application accelerator WAEs, verify that the proper application accelerators, policies, and classifiers are configured. For more information on configuring accelerators, policies, and classifiers, see Chapter 12, "Configuring Application Acceleration" in the *Cisco Wide Area Application Services Configuration Guide*.
- WAAS version 4.1.5x supports SSL application definition, which is enabled for monitoring by default. However, if you are upgrading to version 4.1.5x and already have 20 applications enabled for monitoring, the new SSL application will have monitoring disabled because a maximum of 20 monitored applications are allowed. In order to enable monitoring of the SSL application, you must disable monitoring of a different application and then enable monitoring of the SSL application. You can enable and disable monitoring by using the Enable Statistics check box in the Modifying Application page of the WAAS Central Manager (**Configure > Acceleration > Applications >** *Application Name*).

  If the SSL Bandwidth Optimization chart has no data, then monitoring may be disabled for the SSL application definition. Check that monitoring is enabled for the SSL application.
- WAAS version 4.1.5x supports strong passwords. When you upgrade from version 4.0.17 or an earlier version, which does not support strong passwords, the previous weaker passwords will be retained. For details, see the "Managing Passwords after an Upgrade" section on page 11.
- If you are upgrading a WAAS Central Manager from version 4.0.19 or later and have the secure store enabled, you will need to reopen the secure store after the device reloads (and after any reload). From the WAAS Central Manager GUI, choose **Admin > Secure Store** or use the **cms secure-store open** EXEC command. For more information on using the secure store, see the "Configuring Secure Store Settings" section on page 9-10 in the *Cisco Wide Area Application Services Configuration Guide*.
- If you are upgrading a WAE-511 or WAE-611, ensure that the BIOS disk mode is set to Native.
- When upgrading a WAE from version 4.0.19 or earlier to version 4.1.5x, where the default policy configuration was applied from the CLI, after the upgrade, you may see two classifiers for NFS traffic in the WAAS Central Manager and on the WAE device: NFS and NFS-non-wafs. These classifiers have no effect on NFS traffic acceleration, which continues to operate as configured.
- If you are upgrading from version 4.0.x to version 4.1.x, the way a wildcard mask is interpreted has changed. Wildcard masks can be specified for a traffic classifier match condition or an ACL rule. In version 4.0.x, a wildcard mask of 255.255.255.255 would (incorrectly) match no IP addresses, but in version 4.1.x, this wildcard mask matches any IP address, as expected.

- The device group and role naming conventions have changed in version 4.1.3. Device group and role names cannot contain characters other than letters, numbers, period, hyphen, underscore, and space. (In version 4.0.x, other characters were allowed.) If you upgrade from version 4.0.x to version 4.1.5x, disallowed characters in device group and role names are retained, but if you try to modify the name, you must follow the new naming conventions.
- The standby interface configuration changed in version 4.1.3. If multiple standby groups are configured before upgrading, only the group with the lowest priority and a valid member interface will remain after the upgrade, and it will become standby interface 1. If the errors option was configured, it will be removed.
- If you have two Central Managers that have secure store enabled and you have switched primary and standby roles between the two Central Managers, before upgrading the Central Managers to version 4.1.5x, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords, CIFS file server passwords, and WAFS core passwords. If you do not reenter the passwords, after upgrading to version 4.1.5x, the Central Manager will fail to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you have a version 4.1.1x Central Manager where secure store has been initialized but not opened (such as after a reload) and the Central Manager has sent configuration updates containing user account, CIFS core password, preposition, or dynamic share changes to WAEs before the secure store was opened, then before upgrading the Central Manager to version 4.1.5x, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords, CIFS file server passwords, and WAFS core passwords. If you do not reenter the passwords, after upgrading to version 4.1.5x, the Central Manager will fail to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you have a version 4.1.1x or earlier Central Manager, are using external/remote users that have the admin role, and have edited one or more of these users on the Central Manager, you might encounter caveat CSCsz24694, which causes the Central Manager not to send updates to WAEs after upgrading to version 4.1.5x. To work around this caveat, from the Central Manager, manually edit the external users (without changing anything) after the upgrade. If you have a large number of external users defined, contact Cisco TAC for a script to run before or after the upgrade.

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, reboot the WAE device and wait until the RAID rebuild finishes normally.

Managing Passwords after an Upgrade

WAAS software version 4.1.5x includes a strong password feature for improved security. Versions of the WAAS software previous to 4.0.19 do not have a strong password capability.

Note The following considerations apply to WAAS software version 4.1.5x with the strong password policy enabled. Strong passwords are disabled by default.

When you upgrade from version 4.0.17 or earlier to version 4.1.5x, note the following password considerations:

- Existing passwords from the older version will continue to work in version 4.1.5x.
- 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 8 to 31 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 the characters ' " | (apostrophe, double quote, or pipe) or any control characters.
  - 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.
  - Each new password must be different from the previous 12 passwords.
  - The password cannot contain dictionary words.

Downgrading from Version 4.1.5g to a Previous Version

Note the following guidelines for downgrading:

- Downgrade is supported only to versions 4.1.5f, 4.1.5e, 4.1.5d, 4.1.5c, 4.1.5b, 4.1.5a, 4.1.5, 4.1.3b, 4.1.3, 4.1.1d, 4.0.25, and 4.0.19.

  Note When downgrading from version 4.1.5c or later, dynamic share names with a space are deleted.

- When downgrading WAAS devices, first downgrade application accelerator WAEs, then the standby WAAS Central Manager (if you have one), and lastly the primary WAAS Central Manager.

- If you have a standby WAAS Central Manager, it must be registered to the primary WAAS Central Manager before the downgrade.
- Locked-out user accounts will be reset upon a downgrade.
- All preposition directives configured in CIFS accelerator mode must be removed before downgrading to a version prior to 4.1.1. You also must configure legacy mode file services by enabling a core server and configuring a WAFS core cluster, enabling an edge server, and registering file servers with the Central Manager.
- All dynamic shares configured in CIFS accelerator mode must be switched to legacy mode before downgrading to a version prior to 4.1.1, if you want to keep the dynamic shares. To switch a dynamic share to legacy mode, follow these steps:
  1. Edit the dynamic share in the **Configure > File > Dynamic Shares** window and choose a file server in the drop-down list. (File servers must be previously registered in the **Configure > File > File Servers** window.)
  2. Click **Submit**.

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.1.5f, 4.1.5e, 4.1.5d, 4.1.5c, 4.1.5b, 4.1.5a, 4.1.5, 4.1.3b, 4.1.3, 4.1.1d, 4.0.25, and 4.0.19, follow these steps:

Step 1 (Optional) If secure store is enabled, disable it using the **cms secure-store clear** global configuration command.

```
(config)# cms secure-store clear
```

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 (Optional) If you are downgrading from a fresh install of version 4.1.5 (from the factory or from an installation performed with the WAAS recovery CD), back up the downgrade scripts to an FTP server as follows:

a. Enable FTP on the WAAS Central Manager by using the **inetd enable ftp** global configuration command.

b. Copy the needed downgrade scripts to the FTP server by using the **copy disk** EXEC command, as shown in the following example:

```
CentralManager# copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_5_to_4_1_1d
downgrade/WAAS_Downgrade4_1_5_to_4_1_1d
```

You need to copy only the downgrade scripts that you intend to use. See Step 7 for the complete list of downgrade scripts available.

Step 4 Install the downgrade WAAS software 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 (Optional) If you performed Step 3, then restore the downgrade script files from the FTP server where you backed them up to the /downgrade directory on the WAAS Central Manager by using the **copy ftp** EXEC command as follows:

```
CentralManager# copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_5_to_4_1_1d
downgrade/WAAS_Downgrade4_1_5_to_4_1_1d
```

Step 7 Downgrade the database by using the appropriate **cms database downgrade script** EXEC command.

```
CentralManager# cms database downgrade script downgrade/WAAS_Downgrade4_1_5_to_4_1_1d
```

There are separate scripts depending on what version you are downgrading to:

Note If you are downgrading from version 4.1.5g to version 4.1.5f, 4.1.5e, 4.1.5d, 4.1.5c, 4.1.5b, 4.1.5a, or 4.1.5, no script is necessary. However, you must still execute the **cms database downgrade** command.

- WAAS_Downgrade4_1_5_to_4_0_19
- WAAS_Downgrade4_1_5_to_4_0_25
- WAAS_Downgrade4_1_5_to_4_1_1d
- WAAS_Downgrade4_1_5_to_4_1_3
- WAAS_Downgrade4_1_5_to_4_1_3b

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

```
(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.

Cisco WAE and WAVE Appliance Boot Process

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

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

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

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

- Syslog output contains several instances of the following message:
  "WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device."
- A sysreport and running-config cannot be generated and copied to /local/local1.

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

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

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on cisco.com at the 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 4.1.5x:

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.1.5x devices with devices running earlier software versions.

- WAAS version 4.1.5x does not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.13. If you have any WAAS devices running version 4.0.11 or earlier, you must first upgrade them to version 4.0.13 (or a later version), before you install version 4.1.5x. You should first upgrade any WAEs to version 4.0.13 (or a later version) and then upgrade any WAAS Central Managers to version 4.0.13 (or a later version).
- In a mixed version WAAS network with version 4.1.5x, the WAAS Central Manager must be running the highest version of the WAAS software.

- When a WAAS Central Manager is upgraded to version 4.1.5x and it is managing a 4.0.x device with legacy mode WAFS enabled that is not upgraded, the device may appear to have both legacy mode WAFS and the transparent CIFS accelerator enabled, because the Central Manager enables it by default. Disable the transparent CIFS accelerator if you want to continue to use legacy mode for WAFS.

Configuring Router Buffer Size

Under certain conditions, you may need to increase the IOS buffer size from the default of 18,000 bytes when using mask assignment for load balancing in a WCCP service farm that contains more than 15 WAEs.

You will need to change the buffer size if you see messages similar to the following appearing on the router console:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= <size> -Process= "WCCP V2 Protocol", ipl= 0, pid= <pid>
```

These log messages indicate that the messages being generated are larger than the maximum configured buffer size in IOS. This can occur if a large mask assignment is used in combination with a large number of WAEs in the service group.

The configured IOS buffer size must be larger than the number of bytes reported in the log messages. The maximum configurable IOS buffer size is 65,000 bytes, which you can set with the following IOS command on the routers:

```
Router(config)# buffers huge size 65000
```

- To avoid the need to increase the router buffer size, the number of mask bits set in the WAE WCCP mask assignment configuration can be reduced or the number of WAEs in the farm can be limited. For example, with a default buffer size of 18,000 on the router, a WCCP service group can support 8 WAEs with a mask of 0x7F (7 bits) or 32 WAEs with a mask of 0x7 (3 bits).

Virtual Blade Configuration From File

If you copy the device configuration to the running-config from a file (for example, with the **copy startup-config running-config** command), configuration changes from the file are applied to the device without confirmation. If a virtual blade disk configuration exists in the configuration file and it is different from the actual device configuration, the device virtual blade disk configuration is removed and replaced with the disk configuration from the file. You will lose all data on the virtual blade disks.

Device Group Default Settings

When you create a new device group in WAAS version 4.1.5x, the **Configure > Acceleration > DSCP Marking** page is automatically configured for the group, with the default DSCP marking value of copy.

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 4.1.5g Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5g:

Software Version 4.1.5g Resolved Caveats

The following caveats were resolved in software version 4.1.5g.

Caveat ID Number	Description
CSCsz09603	Java heap OutOfMemory errors were observed in WAE rarely under stress

Software Version 4.1.5g Open Caveats

The open caveats for software version 4.1.5g are the same as those for software version 4.1.5f. For details, see the "Software Version 4.1.5f Open Caveats" section.

Software Version 4.1.5f Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5f:

Software Version 4.1.5f Resolved Caveats

The following caveats were resolved in software version 4.1.5f.

Caveat ID Number	Description
CSCtg28040	File Save/Save As Issues After Installing Microsoft Patch (KB980232)

Software Version 4.1.5f Open Caveats

The open caveats for software version 4.1.5f are the same as those for software version 4.1.5e, with the exception of CSCtg28040, which is resolved for 4.1.5f. For details, see the "Software Version 4.1.5e Open Caveats" section.

Software Version 4.1.5e Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5e:

Software Version 4.1.5e Resolved Caveats

The following caveats were resolved in software version 4.1.5e.

Caveat ID Number	Description
CSCtc38791	'Citrix Shadowing' tool may experience slowness with CIFS AO enabled
CSCtd60963	MS Word "Save as" with offline files may not work in a specific case
CSCte61998	CMS service restarts after a long period due to slow memory leak

Software Version 4.1.5e Open Caveats

The following open caveats apply to software version 4.1.5e.

Caveat ID Number	Description
CSCtb33915	Device reboots after tethereal run for many hours
CSCte72709	CIFS/Print: stapling/duplex printing for Canon driver makes Conn fail
CSCte98452	Samba client writes may fail on Samba server with specific POSIX ext
CSCtf02867	Due to rare JVM crash, Jave core file gets generated on CM
CSCtf31614	In rare case, CifsAO can cause a core file to be created

The additional open caveats for software version 4.1.5e are the same as those for software version 4.1.5d, with the exception of CSCtc38791 and CSCtd60963, which are resolved for 4.1.5e. For details, see the "Software Version 4.1.5d Open Caveats" section.

Software Version 4.1.5d Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5d:

Software Version 4.1.5d Resolved Caveats

The following caveats were resolved in software version 4.1.5d.

Caveat ID Number	Description
CSCsw17984	Removal/replacement of policies does not work if DSCP configured for app
CSCsy24825	With customized time zone config, syslog has mismatch in time stamp
CSCta42125	CM may report "Driver Invalid for distribution" message after upgrade
CSCtb05448	SNMP triggers may be deleted after reload of WAE
CSCtb74241	In a rare case scenario HTTP connection may fail with inline mode
CSCtc58064	WAE device may send statistics to CM after deactivation
CSCtc86937	CM may not be able to list custom reports created by deleted users
CSCtd56787	"show statistics connection" CLI times out in a specific scenario
CSCtd81847	Printing works only for 'Domain Administrator' account after WAE upgrade

Software Version 4.1.5d Open Caveats

The following open caveats apply to software version 4.1.5d.

Caveat ID Number	Description
CSCtd19677	In rare case, WAE-7326 power monitoring impacts performance
CSCtd67970	WAE stops WCCP processing in a rare scenario
CSCte19330	Under rare scenario WAE may stop optimizing traffic and reload
CSCte42826	Pagination not working in the print drivers page.

The additional open caveats for software version 4.1.5d are the same as those for software version 4.1.5c, with the exception of CSCsw17984, CSCtb74241, CSCtc58064, CSCtc86937, CSCtd56787, and CSCtd81847, which are resolved for 4.1.5d. For details, see the "Software Version 4.1.5c Open Caveats" section.

Software Version 4.1.5c Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5c:

Software Version 4.1.5c Resolved Caveats

The following caveats were resolved in software version 4.1.5c.

Caveat ID Number	Description
CSCsv17468	WCCP shutdown taking longer than configured timeout
CSCsx96126	Exception if no share or "/" used as root for CIFS preposition (CLI/CM)
CSCsy01801	CM: Schedule changes for PP not taking effect intermittently
CSCsz31059	Rarely, CIFS-AO service disabled alarm seen on NME-502 after upgrade
CSCta06901	Samba clients talking to Samba server may see directory browsing errors
CSCtb27331	CIFS AO edge WAE may not return File Stream Info response to the client
CSCtb43432	Under certain conditions prepositions tasks may be deleted and added
CSCtb58739	Rarely, WAE running config may be overriden with start-up config
CSCtb68165	Pagination not working while changing the number of rows from last page
CSCtb81842	Under heavy load, DRE process may generate core file
CSCtb88170	Rarely device GUI may not be accessible after reload
CSCtb89492	WAAS: Preposition task may fail due to resources being unavailable
CSCtb92703	PsExec application from Windows client fails when CIFS AO is enabled
CSCtc14960	SNMP process may cause high CPU under heavy traffic load
CSCtc85179	After transferring > 2 GB of a file with CIFS AO, the transfer may slow

Software Version 4.1.5c Open Caveats

The following open caveats apply to software version 4.1.5c.

Caveat ID Number	Description
CSCtc75606	In rare scenario CIFS AO may encounter out of memory error
CSCtc86937	CM may not be able to list custom reports created by deleted users
CSCtd42371	Communication between CM and WAE is broken after restoring CM db backup
CSCtd50754	Device CMS may fail to process configuration updates from CM
CSCtd56466	WAFS: under rare circumstances a java core file may be created
CSCtd56787	showstatistics connection CLI times out in a specific scenario
CSCtd56874	In a specific case an incomplete configuration may be applied to the WAE
CSCtd60131	Device reporting alarm "actastor_watchdog service has been disabled"
CSCtd60963	MS Word "Save as" with offline files may not work in a specific case
CSCtd68080	DRE messages occasionally flooding syslog
CSCtd70016	Under rare circumstances, after reload, CIFS AO can not be re-enabled
CSCtd71211	Under certain conditions can not create preposition from pre 4.1.5c WAE
CSCtd81847	WAAS Printing does not work unless the user is a Domain Administrator

The additional open caveats for software version 4.1.5c are the same as those for software version 4.1.5b, with the exception of CSCsz31059, CSCtb27331, CSCtb43432, and CSCtb58739, which are resolved for 4.1.5c. For details, see the "Software Version 4.1.5b Open Caveats" section.

Software Version 4.1.5b Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5b:

- Software Version 4.1.5b Resolved Caveats
- Software Version 4.1.5b Open Caveats

Software Version 4.1.5b Resolved Caveats

The following caveats were resolved in software version 4.1.5b.

Caveat ID Number	Description
CSCtb10199	Unable to change a Standby Interface to Primary in particular scenario
CSCtb52141	Central Manager CMS service may restart in certain scenarios
CSCtb55631	Outlook may experience slow response in rare cases
CSCtb88451	File open may fail with certain NAS with non standard CIFS
CSCtc14293	Outlook client unresponsive while copying private sub-folders to public

Software Version 4.1.5b Open Caveats

The following open caveats apply to software version 4.1.5b.

Caveat ID Number	Description
CSCtc38791	'Citrix Shadowing' tool may experience slowness with CIFS AO enabled
CSCtc39508	WAVE configured as a standby group may lose connectivity after upgrade
CSCtc52362	ssh access to Windows on Virtual Blade may not work
CSCtc58064	WAE device may send statistics to CM after deactivation

The additional open caveats for software version 4.1.5b are the same as those for software version 4.1.5, with the exception of CSCtb52141, CSCtb55631, and CSCtb88451, which are resolved for 4.1.5b. For details, see the "Software Version 4.1.5 Open Caveats" section.

Software Version 4.1.5a Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.5a:

- Software Version 4.1.5a Resolved Caveat
- Software Version 4.1.5a Open Caveats

Software Version 4.1.5a Resolved Caveat

The following caveat was resolved in software version 4.1.5a.

Caveat ID Number	Description
CSCtc20871	Under specific scenario, user may need to retry CIFS file access

Software Version 4.1.5a Open Caveats

The open caveats for software version 4.1.5a are the same as those for software version 4.1.5. For details, see the "Software Version 4.1.5 Open Caveats" section.

Software Version 4.1.5 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.1.5:

Software Version 4.1.5 Resolved Caveats

The following caveats were resolved in software version 4.1.5.

Caveat ID Number	Description
CSCsu79483	"sh cifs session list" doesnt work in Legacy with Edge + Core cfg on WAE
CSCsv40789	Tethereal read filter is not applied if capture data is written to file
CSCsv65297	Rarely communication between Win98 clients and print servers may fail
CSCsw94689	OS/2 clients cannot access file server when using CIFS AO
CSCsx26086	Incorrect assignments on WAE's when lead WAE joins an unstable farm
CSCsx40169	Traffic redirected to the WAE may get dropped under certain conditions
CSCsx74221	Directed Mode with GRE return may cause high cpu utilization on routers
CSCsy21549	CM data base backup fails if print related config files are corrupted.
CSCsy26868	Interface counters did not increase after reaching the max value
CSCsy29150	Upon WAE leaving wccp farm, remaining WAE connections can get reset
CSCsy50180	Device group policy definition is overridden under certain conditions
CSCsy58389	TACACS attribute configuration with symbol '*' is ignored by CM GUI
CSCsy68972	Rescue CD installs binary image on incompatible RAID drive

Caveat ID Number	Description
CSCsy70855	WAE may generate a dataserver core file for a WAFS statistics request
CSCsz09584	Cannot add remote user names starting with numeric character
CSCsz21500	Windows Domain NetBios name changes may not register with WINS server
CSCsz22079	In very rare cases, Outlook clients may need to reconnect
CSCsz25404	Some CIFS AO expert-mode configuration is not persistent
CSCsz31354	Under rare scenario user may need to retry file access with SMB signing
CSCsz65548	CIFS server initiated request may experience slow response in some cases
CSCsz72205	Switching device in CIFS acceleration report on CM may result in error
CSCsz72423	WAAS print services not refreshing printers DNS entries
CSCsz77782	Outlook calendar may experience slow response in some cases
CSCsz79689	WAE creates kdump file and reboots in special condition
CSCsz81991	CMS generated core under certain circumstance
CSCsz87027	In rare cases, SNMP client may need to retry requests
CSCsz89679	Tethereal termination for rolling captures may fail
CSCta03256	Client side WAE drops SYN-ACK with its own Device ID in TCP Option
CSCta06947	Slow Performance with CIFS-AO with very large PST files across WAN
CSCta07598	CIFS-AO truncates READ response if the READ request received is > 65535
CSCta18195	HTTPS Proxy connections may get reset with mixed 4.1.1 and 4.1.3 WAAS
CSCta21795	Rarely WAE could kdump and reboot during internal connection setup
CSCta27573	Under certain conditions, config update between CM and WAE may fail
CSCta43610	Under certain conditions, outlook client may experience slow reseponse
CSCta47695	Remote installations failed using HP PXE boot client with cifsao enabled
CSCta77941	WAE loses static routes when Standby interface members removed and added
CSCta94350	Under rare conditions, CM key manager may fail to serve keys to WAEs.
CSCtb06440	In rare cases video connection may get reset during setup phase

Software Version 4.1.5 Open Caveats

The following open caveats apply to software version 4.1.5.

Caveat ID Number	Description
CSCsr48090	LZ compression errors may be seen with video traffic under heavy load
CSCsv79687	Under rare conditions, 'actastor_watchdog' alarm raised and cleared
CSCsw17984	Removal/replacing Acceleration Device Group parameters does not work
CSCsx22929	Outlook2K clients can't move group of mails between folders with MAPI AO
CSCsx58948	Connections initiated by external Backup Applications may not succeed
CSCsx66071	Preposition task may be started randomly assuming a wrong time zone

Caveat ID Number	Description
CSCsx78566	Under rare conditions, cannot delete dynamic shares from the CM
CSCsy19941	Scheduled report generation may fail under certain conditions.
CSCsy31216	Incorrect reference count is displayed after concurrent CIFS traffic
CSCsy47877	Zero buckets were allocated on upgrade from 4.1.1c to 4.1.3 on NM
CSCsy99732	In rare cases duplicate emails or send failures may be seen
CSCsz18986	CIFS-AO: Remote Windows installation using MS-DOS client fails
CSCsz31059	Rarely, CIFS-AO service disabled alarm seen on NME-502 after upgrade
CSCsz74594	Outlook may fail to connect under rare overload cases
CSCsz79863	Preposition task may fail to fetch all files after network disruption
CSCta08640	Server may deny access to share via CIFS AO
CSCta36302	In extreme conditions device may go offline losing network connectivity
CSCtb12760	Device may become unresponsive due to nscd lockup
CSCtb13415	Core file may be generated resetting HTTP connections in a rare scenario
CSCtb27331	CIFS AO edge WAE may not return File Stream Info response to the client
CSCtb36731	WAE may try secondary server even after primary rejects authentication
CSCtb43432	Under certain conditions prepositions tasks may be deleted and added
CSCtb52141	Central Manager CMS service may restart in certain scenarios
CSCtb55631	Outlook may experience slow response in rare cases
CSCtb58739	Rarely, WAE running config may be overriden with start-up config
CSCtb74241	SYN from reused HTTP session may be dropped in specific linline mode
CSCtb85564	WAAS NTP authentication may not succeed in some cases
CSCtb88451	File open may fail with certain NAS with non standard CIFS

Software Version 4.1.5 Command Changes

This section lists the new and modified commands in WAAS software version 4.1.5.

Table 1 lists the new commands and options that have been added in WAAS software version 4.1.5.

Table 1 CLI Commands Added in Version 4.1.5

Mode	Command and Syntax	Description
EXEC	**clear statistics snmp**	Clears the SNMP statistics.

Table 2 lists existing commands that have been modified in WAAS version 4.1.5.

Table 2 CLI Commands Modified in Version 4.1.5

Mode	Command and Syntax	Description
EXEC	**clear arp-cache interface**	Removed values 2, 3, and 4 from the **standby** option.
	crypto import ca-certificate	DSA certificates and keys cannot be imported.
	show cdp	Added values 3 and 4 to the **inlineport** option.
	show statistics accelerator http	Added the following counter to the command output: "Total number of AO SYN handling timeouts"
	show statistics accelerator ssl	Added the following counter to the command output: "Number of flows deleted due to timeout in rehandshake"
	show statistics auto-discovery	Added the following counters to the command output: "SYN-ACKs found with our device id" "SYN-ACKs found with mirrored options"
	show statistics connection	Added the following counters to the command output: "Current Reserved Flows" "RR" Current Reserved Flows shows the connections reserved for the MAPI accelerator. It appears for all accelerators. Reduction Ratio (RR) shows the relative reduction ratio (in bytes) for a particular connection.
	show statistics connection closed	Added summary and detailed flow statistics per flow reduction ration (savings) counters to the **dre last detail** option command output.
	show snmp event	Added the following field to the command output: "Wildcard"
	show statistics tfo	Modified the "Connections queued for accept" command output counter to "Total Connections queued for accept." The total connections is a cumulative count, not a current count.
	show tfo detail	Added the following counter to the command output: "Effective Limit" Effective Limit shows the connections remaining of the Connection Limit less the Current Reserved Flows.
	test self-diagnostic	Added the **application-security** option.
Global configuration	**ip access-list**	Added **logging** option to enable/disable IP ACL logging of denied packets.
	snmp-server trap-source	Removed values 2, 3, and 4 from the **standby** option.
	no windows-domain	Removed the argument *name* from the **netbios-name** option.

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 Services API Reference*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *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 Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 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*
- *Regulatory Compliance and Safety Information for the Cisco Content Wide Area Virtualization Engines*

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.

This document is to be used in conjunction with the documents listed in the "WAAS Documentation Set" section.