Release Note for Cisco Wide Area Application Services Software Version 4.3.1x

October 29, 2012

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:

- 4.3.1

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 4.3.1:

Software Version 4.3.1 New and Changed Features

WAAS software version 4.3.1 includes the following new features and changes:

- vWAAS—Virtual WAAS appliance support allows you to quickly deploy vWAAS devices on VMWare ESXi hosts such as the Cisco Unified Computing System (UCS), and interoperates with the Nexus 1000V Switch. The WAAS Central Manager can manage vWAAS devices in the same integrated graphical interface through which it manages other WAAS devices in the network. In addition, the vWAAS Central Manager (vCM) can be deployed in a virtual appliance form factor, providing central management for both physical and virtual Cisco WAAS instances. See the new *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide* for details.

  If you are interoperating with the Nexus 1000V Switch, vWAAS requires Nexus 1000V release 4.2.1SV1(4).

- WAAS Express Central Manager support—The WAAS Central Manager can manage WAAS Express software running on Cisco ISR G2 routers in the same integrated graphical interface through which it manages other WAAS devices in the network.

  WAAS Express requires IOS release 15.1(3)T on the Cisco ISR G2 router.

- HTTPS Application Acceleration—The HTTP and SSL application accelerators are enhanced to better support the HTTPS protocol.

- Monitoring and Reporting—New Summary and Connection Trend reports simplify WAAS network monitoring. A new HTTPS Acceleration report displays HTTPS traffic acceleration statistics. A new Throughput report displays inbound and outbound device throughput statistics.

- SNMP—Support for the IF-MIB is added.

- CLI commands—For CLI command changes, see the "Software Version 4.3.1 Command Changes" section on page 17.

- Monitoring API—For API changes, see the "Software Version 4.3.1 Monitoring API" section on page 18.

Software Version 4.3.1 Filenames

WAAS software version 4.3.1 includes the following software image files for use on WAAS appliances and modules:

Standard Image Files

WAAS software version 4.3.1 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-4.3.1.*x*-k9.bin—Universal software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device.
- waas-accelerator-4.3.1.*x*-k9.bin—Application Accelerator software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device, including those on a SM-SRE module. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator-only image.
- waas-sre-installer-4.3.1.*x*-k9.zip—SM-SRE install zip file that includes all the files necessary to install WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-4.3.1.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-4.3.1.*x*-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-274/474/574 and WAE-674/7341/7371 devices).
- waas-4.3.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.3.1.*x*-k9.bin—Kdump analysis component that you can install and use with the Application Accelerator software image.
- waas-alarm-error-books-4.3.1.*x*.zip—Contains the alarm and error message documentation.
- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available under the Cisco Wide Area Application Services (WAAS) Software > Tools directory on Cisco.com.)

No Payload Encryption (NPE) Image Files

WAAS software version 4.3.1 includes NPE primary software image files that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. NPE primary software image files include the following:

- waas-universal-4.3.1.*x*-npe-k9.bin—Universal NPE software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade either a Central Manager or an Application Accelerator device.
- waas-accelerator-4.3.1.*x*-npe-k9.bin—Application Accelerator NPE software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device, including those on a SM-SRE module. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator only image.

- waas-sre-installer-4.3.1.*x*-npe-k9.zip—SM-SRE install zip file that includes all the NPE files necessary to install WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-4.3.1.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-4.3.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-274/474/574 and WAE-674/7341/7371 devices).
- waas-4.3.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.3.1.*x*-npe-k9.bin—NPE Kdump analysis component that you can install and use with the Application Accelerator software image.
- waas-alarm-error-books-4.3.1.*x*-npe.zip—Contains the NPE alarm and error message documentation.
- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available under the Cisco Wide Area Application Services (WAAS) Software > Tools directory on Cisco.com.)

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:

WCCP Interoperability

Central Managers running version 4.3.1 can manage WAEs running software versions of 4.0.19 and later. However, it is recommended that all WAEs in a given WCCP service group be running the same version.

Note The default value for the WCCP source IP mask changed in version 4.2.1 to 0xF00. If you are upgrading a WAE that previously used the default WCCP source IP mask of 0x1741, its WCCP mask is not changed. Note that all WAEs in a WCCP service group must have the same mask.

To upgrade the WAEs in your WCCP service group, 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 Perform the WAAS software upgrade on all WAEs using the WAAS Central Manager GUI.

Step 3 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 4 If mask assignment is used for WCCP, ensure that all WAEs in the service group are using the same WCCP mask value.

If you have upgraded any WAEs from a version earlier than 4.2.1, and the WAEs were using the default mask value, the mask value is not changed by the upgrade.

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
```

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, follow these 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 previous 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

Upgrading from a Prerelease Version to Version 4.3.1

To upgrade from WAAS prerelease software to version 4.3.1, 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 a Release Version to Version 4.3.1

This section contains the following topics:

For additional upgrade information and detailed procedures, refer to the *Cisco Wide Area Application Services Upgrade Guide*.

Requirements and Guidelines

When you upgrade to version 4.3.1, observe the following guidelines and requirements:

- Upgrading to version 4.3.1 is supported only from versions 4.0.19, 4.0.27, 4.1.1d, 4.1.3, 4.1.3b, 4.1.5c, 4.1.5f, 4.1.7a, 4.2.1, 4.2.3, and 4.2.3b. If you want to upgrade a WAAS device running a different version, first upgrade to the next supported version in the list, and then upgrade to the current 4.3.1 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 4.3.1, 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 4.3.1 using the **Jobs > Software Update** page from a 4.0.x WAAS Central Manager, enter 4.3.1.0.1 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 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 the "Configuring Application Acceleration" chapter in the *Cisco Wide Area Application Services Configuration Guide*.
- WAAS version 4.3.1 supports SSL application definition, which is enabled for monitoring by default. However, if you are upgrading from version 4.1.1 or earlier to version 4.3.1 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, monitoring may be disabled for the SSL application definition. Check that monitoring is enabled for the SSL application.
- 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 in the *Cisco Wide Area Application Services Configuration Guide*.
- When upgrading a WAE from version 4.0.19 to version 4.3.1, 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 or later, 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 and later, this wildcard mask matches any IP address, as expected.
- The device group and role naming conventions 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 4.3.1, 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 from version 4.1.1 or earlier, 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 4.3.1, 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 4.3.1, the Central Manager fails 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 4.3.1, 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 4.3.1, the Central Manager fails 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.
- The default value for the WCCP source IP mask changed in version 4.2.1 to 0xF00. If you are upgrading a WAE that previously used the default WCCP source IP mask of 0x1741, its WCCP mask is not changed. Note that all WAEs in a WCCP service group must have the same mask. For the recommended upgrade procedure for WAEs in a service group, see the "WCCP Interoperability" section on page 5.
- The SNMP username and remote entity ID constraints changed in version 4.2.1. SNMP usernames are limited to 32 characters. (In version 4.1x and earlier, 64 characters were allowed.) SNMP remote entity IDs must be between 10-32 hexadecimal characters. (In version 4.1x and earlier, 1-64 characters were allowed.) If you upgrade from version 4.1x or earlier to version 4.3.1, invalid settings in these fields are deleted.
- Central Manager support for configuring the Initial Slow Start Threshold TCP/IP setting was removed in version 4.2.1. If your Central Manager is managing devices earlier than version 4.2.1, you may see repeated device configuration change updates for the Initial Slow Start Threshold configuration parameter coming from these devices when this parameter is assigned a non-default value in the devices. To avoid these repeated updates, use the **no tcp init-ss-threshold** global configuration command to set the default value on the devices, which is the recommended value for most networks.
- If you are upgrading a Central Manager from version 4.1.1x to version 4.3.1, before you upgrade, save all scheduled default reports that exist in version 4.1.1x to avoid failed scheduled reports. To save a default report that you want to schedule, display the report and click the **Save** button. This requirement does not apply if you are upgrading from 4.1.3 or later because default reports are automatically saved.
- If you are upgrading a Central Manager from version 4.2.3x or earlier to version 4.3.1, and you have any scheduled reports that are configured for more than 100 recurrences, after the upgrade only 100 recurrences are retained.

- After upgrading a Central Manager from version 4.1.x to version 4.3.1, any scheduled reports that contain the following charts are removed from the Manage Reports and Scheduled Reports lists: Managed Devices Information, CPU Utilization, and any CIFS charts. You can reschedule the CPU Usage report for a device if you want. The Managed Devices and CIFS charts are not applicable as part of a scheduled report.
- After upgrading a Central Manager from version 4.1.1x to version 4.3.1, any scheduled reports that are pending (not yet completed) are removed. To continue generating these reports, reschedule them.
- If you use the setup utility for basic configuration after upgrading to 4.3.1, wccp router list 7 is used. Since the setup utility is designed for use on new installations, any existing configuration for wccp router list 7 will be replaced with the new configuration.
- If you have disk encryption enabled and are upgrading to version 4.3.1 NPE from version 4.2.1 or earlier, disk encryption configuration as well as disk cached data are lost. There is no impact when upgrading to standard version 4.3.1 (non-NPE).
- Beginning with version 4.3.1, the print admin role is no longer assigned to all admin user accounts by default. However, if you are upgrading from an earlier version, the print admin role is not automatically removed from all admin user accounts. To manually remove the print admin role from an account, edit the admin user from the **Admin > AAA > Users** page, uncheck the Print Admin check box, and click **Submit**.
- After upgrading a Central Manager to version 4.3.1, the AllDevicesGroup device group is renamed to the AllWAASGroup. Additionally, an AllWAASExpressGroup is created for all WAAS Express devices.

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.

Downgrading from Version 4.3.1 to a Previous Version

Note the following guidelines for downgrading:

- Downgrade is supported only to versions 4.2.3b, 4.2.3, 4.2.1, 4.1.7a, 4.1.5f, 4.1.5c, 4.1.3b, 4.1.3, 4.1.1d, 4.0.27, or 4.0.19.
- On a vWAAS device you cannot downgrade to a version earlier than 4.3.1.
- 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.
- When downgrading from a WAAS NPE version to a version earlier than 4.2.3, the **show version last** command does not display NPE in the version output.
- If two Cisco WAE Inline Network Adapters are installed in a WAE, you must remove one of the adapters before you downgrade the WAE to a version earlier than 4.2.1. Two Cisco WAE Inline Network Adapters are not supported in WAAS versions earlier than version 4.2.1.
- If downgrading to version 4.2.1, you must first change the password for WCCP, SNMP user, RADIUS, TACACS, or transaction log modules before the downgrade if any of the special characters !@#$%\ were used in the password for the module. Otherwise, the related CLI commands for those modules will fail.
- Due to stricter security implemented in version 4.2.1 and later, when downgrading to a version earlier than 4.2.1, any configuration settings that contain passwords or security keys are discarded and will have to be reconfigured. Affected CLI commands include the following: **ntp**, **radius-server**, **snmp-server user**, **tacacs**, **transaction-logs**, and **wccp tcp-promiscuous router-list-num**. After the downgrade, discarded configurations are listed in the file /local1/discarded_cli.

  Additionally, the following Central Manager settings are affected:

  - All SNMP users are deleted.
  - The RADIUS encryption key is deleted.
  - The TACACS security word is deleted.
  - The Email notification server password is deleted.
  - The transaction log and video acceleration transaction log export server configurations are deleted.
  - The WCCP password is set to null.
  - The username and password (if defined) associated with all software image files is set to anonymous/anonymous.
- 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 earlier than 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 earlier than 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**.
- If extended object cache is enabled, all CIFS cache data, DRE cache data, and virtual blade data is lost when downgrading to a version earlier than 4.2.1.
- Any new reports and charts that were introduced in version 4.3.1 are removed from managed reports and scheduled reports when downgrading to an earlier version.
- The default value for the WCCP source IP mask changed in version 4.2.1 to 0xF00. If you are downgrading a 4.3.1 WAE that uses the default WCCP source IP mask, its WCCP mask is not changed on downgrade to a version earlier than 4.2.1. Note that all WAEs in a WCCP service group must have the same mask.
- If you use the setup utility for basic configuration after downgrading to a version earlier than 4.2.3x, WCCP router list 8 is used. Since the setup utility is designed for use on new installations, any existing configuration for WCCP router list 8 will be replaced with the new configuration.
- After downgrading a Central Manager to a version earlier than 4.3.1, the AllWAASGroup device group is renamed to the AllDevicesGroup. Additionally, the AllWAASExpressGroup is removed.
- After downgrading a Central Manager to a version earlier than 4.3.1, all registered WAAS Express devices are deleted from the Central Manager. If the Central Manager is later upgraded to 4.3.1, WAAS Express devices must be registered again.

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

Step 1 If you are downgrading to version 4.1.1x or earlier and the secure store is enabled in the Central Manager, disable it using the **cms secure-store clear** global configuration command. (This step is not needed if you are downgrading to version 4.1.3 or later.)

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

Step 2 (Optional) From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device.

```
CentralManager# cms database backup
```

Step 3 Install the downgrade WAAS software image by using the **copy ftp install** EXEC command.

Step 4 Reload the device.

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 4.3.1:

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.3.1 devices with devices running earlier software versions.

- WAAS version 4.3.1 does not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.19. If you have any WAAS devices running version 4.0.17 or earlier, you must first upgrade them to version 4.0.19 (or a later version), before you install version 4.3.1. You should first upgrade any WAEs to version 4.0.19 (or a later version) and then upgrade any WAAS Central Managers to version 4.0.19 (or a later version).
- In a mixed version WAAS network with version 4.3.1, the WAAS Central Manager must be running the highest version of the WAAS software.
- When a WAAS Central Manager is upgraded to version 4.3.1 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 on the 4.0.x device.

Central Manager Report Scheduling

In the WAAS Central Manager, we recommend running system wide reports in device groups of 250 devices or less, or scheduling these reports at different time intervals, so multiple system wide reports are not running simultaneously.

WAAS Express Policy Changes

Making policy changes to large numbers of WAAS Express devices from the Central Manager may take longer than making policy changes to WAAS devices.

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 device group in WAAS version 4.3.1, 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.

Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP

When using the Cisco ASR 1000 Series router and WCCP to redirect traffic to a WAE that is using WCCP GRE return as the egress method and the HTTP accelerator is enabled, there may be an issue with HTTP slowness due to the way the ASR router handles proxied HTTP connections (see CSCtj41045). To work around this issue, on the ASR router, create a web cache service in the same VRF as that of the 61/62 service by using the following command: **ip wccp [vrf** *vrf-name***] web-cache**

Internet Explorer Certificate Request

If you use Internet Explorer to access the Central Manager GUI version 4.3.1 or later and Internet Explorer has personal certificates installed, the browser prompts you to choose a certificate from the list of those installed in the personal certificate store. The certificate request occurs to support WAAS Express registration and is ignored by Internet Explorer if no personal certificates are installed. Click **OK** or **Cancel** in the certificate dialog to continue to the Central Manager log in page. To avoid this prompt, remove the installed personal certificates or use a different browser.

Software Version 4.3.1 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.3.1:

Software Version 4.3.1 Resolved Caveats

The following caveats were resolved in software version 4.3.1.

Caveat ID Number	Description
CSCsx64796	CIFS AO may generate core on large print jobs while low on memory
CSCtb29132	Upgrade failure can happen in rare scenario
CSCtc38874	"License Transport not been purchased" error message is displayed
CSCte72709	CIFS/Print: stapling/duplex printing for Canon driver makes Conn fail
CSCte98452	CIFS: Samba clients talking to Samba server can't write or copy files
CSCtf23512	Connections break with http optimizer when server starts protocol mesgs
CSCtf87641	Rarely MAPI AO may restart causing Outlook to re-establish connections
CSCth17470	User unable to access CIFS share because CIFS AO not close search handle
CSCth52870	HTTPS: Core file generated on edge WAE on 1 GB file download
CSCth65564	MAPI AO may restart during load
CSCth72473	Windows Active Directory registration not successful from CM GUI
CSCth79547	WAE creates KDUMP file and reboot while handling bi-directional traffic
CSCth83497	SSL traffic does not get established if domain server and proxy is confi
CSCti00279	In rare case WAE repeatedly fails to connect to CM, shows offline
CSCti00877	WEXP device goes offline in CM GUI on deleting a Application policy
CSCti05481	standby CM OutofMem due to growing ao_stats_collection_info table
CSCti05931	CIFS AO: file browsing may fail when user password exceeds 14 characters
CSCti10857	CM Audit log missing info from Device / Device Group assignment page
CSCti25420	Device goes to debugshell while installing image from Rescue CD
CSCti30071	so_dre process got stuck in zombie state
CSCti30954	WAAS NM-WAE configuration is only loaded partially after a reboot.
CSCti33775	preposition not applied to devices if schedule set before assign devices
CSCti37131	NM-WAE manufacture failed

Caveat ID Number	Description
CSCti39812	Proxy CONNECT request doesn't get established with SSL version mismatch
CSCti40797	Can not remove Print Admin from admin username on CM after 4.2.1 upgrade
CSCti44815	so_dre creates core during low CC test
CSCti52342	SSLcore file created and conn not closed after long duration mix ao load
CSCti65036	Rescue CD does not work through serial console
CSCti67679	SM 900 optimizes more connections than the connection limit specified
CSCti72723	WAAS - DRE should check sync messages for proper peer ID
CSCti73800	CM registration failed when router cert exceeds certain size
CSCti77492	Kernel crash was seen in SM900 when running stress tests
CSCti84213	Cross-Site Scripting Vulnerabilities in Several Management Pages
CSCti96990	Samba security update
CSCtj18726	HW-RAID platforms can lose partition table during disk stress & CTRL+C
CSCtj60153	WAE upgrade from 421b38 to 4.3.0b91 does not restore to online.
CSCtj63555	MAC address of physical interface changes upon start of virtual blade

Software Version 4.3.1 Open Caveats

The following open caveats apply to software version 4.3.1.

Caveat ID Number	Description
CSCsj95489	Client throws error during Big file copy
CSCsq38730	CR disk_failure alarm was cleared after reloading and power cycling
CSCsr88316	WAFS Edge or CIFS-AO restarts due to false liveliness alarm
CSCsu08094	Force Device Group icon appears in device group config on upgrade
CSCsu65901	In a rare scenario, java corefile seen on a 274 WAE running HTTP traffic
CSCsv79472	CIFS AO may restart due to liveliness alarm
CSCsw82237	"wafs_edge_down" alarm raised during non CIFS load test
CSCsx37440	CM GUI:Not able to resize the charts in particular scenario.
CSCta05256	cifs liveliness error messages encountered-cifs servc dead alarms
CSCtb82059	CM - Upgrade JVM deployed with WAAS to 1.6
CSCtb99184	connections through NFS AO may get reset under some rare scenarios
CSCtd70016	Under rare circumstances, after reload, CIFS AO can not be re-enabled
CSCtd78714	Disabling WCCP from CM causes few commands reconfig upon submit
CSCtf02867	Due to rare JVM crash, java core file gets generated on CM.
CSCtf03624	Big file copy may fail with vista client with cifsao
CSCtf06224	Tethereal packet capture aborted in a specific case
CSCtf31614	In rare case, CifsAO can cause a core file to be created

Caveat ID Number	Description
CSCtf54766	Errors observed when SSL is not optimizing connections in rare scenarios
CSCtf83578	IP address missing in CM after cms database restore
CSCtf97106	CIFS acceleration reports graph may show value of '1' always
CSCtg05509	Do not apply ACL for the transit traffic, when it applied on Gig x/0
CSCtg11210	Mask value is not removed on overriding WCCP Device Group settings
CSCtg36847	Changing write-caching policy not allowed on virtual-blade hard disks
CSCtg76013	Overriding Group settings is removing some snmp settings.
CSCtg89763	SETUP on NM/SM should check the router user privilege
CSCth07448	Rarely under heavy stress test, WAVE-574 disk failure may occur
CSCth07637	Rarely under heavy stress test, WAVE-474 disk failure may occur
CSCth07735	Rarely, policy configurations removed from the WAE
CSCth08362	Rarely, WAE sending all configs to CM leading to re-application of CLIs
CSCti20838	Modification of interface ACL via CM caused traffic drop
CSCti29135	RBAC:Not able to create new appln/classifiers in Policy Prioritization
CSCtj00911	In rare cases, DRE hints stat may be incorrect when SSLAO is overloaded
CSCtj05828	Security vulnerabilities in Apache server code used in WAAS
CSCtj28535	Invalid pop-up raised when register to windows domain with apply default
CSCtj42030	WAE 612 reloaded after creating kdump file
CSCtj43510	MAPI AO may create core dump under rare circumstances of disconnects
CSCtj49204	CM GUI blocking to create remote AAA users when users in transient cache
CSCtj52999	Java Exceptions seen when updating peer settings
CSCtj70186	SSL pages are going to override mode in specific scenario

Software Version 4.3.1 Command Changes

This section lists the new and modified commands in WAAS software version 4.3.1.

Table 1 lists the commands and options that have been added in WAAS version 4.3.1.

Table 1 CLI Commands Added in Version 4.3.1

Mode	Command	Description
EXEC	**clear cache http-metadatacache https**	Added the **https** option, which clears the HTTPS metadata cache.
	clear statistics vn-service vpath	Clears vWAAS VPATH statistics.
	show statistics vn-service vpath	Displays vWAAS VPATH statistics.
	vm	Initializes a vWAAS virtual machine after a VMWare cloning operation, or synchronizes the vWAAS clock with the host. Available only on vWAAS devices.

Table 1 CLI Commands Added in Version 4.3.1 (continued)

Mode	Command	Description
Global configuration	**ip icmp rate-limit unreachable**	Sets the rate at which ICMP destination unreachable messages are generated.
	ip unreachables df	Disables or enables the ICMP unreachable feature.
	interface virtual	Creates a virtual interface on a vWAAS device.
	vn-service vpath	Enables or disables VPATH interception on a vWAAS device.

Table 2 lists existing commands that have been modified in WAAS version 4.3.1.

Table 2 CLI Commands Modified in Version 4.3.1

Mode	Command	Description
EXEC	**clear cache http-metadatacache https**	Added the **https** option, which clears the HTTPS metadata cache.
	show cache http-metadatacache https	Added the **https** option, which displays HTTPS metadata cache entries.
	show interface virtual	Added the **virtual** option, which displays virtual interface device information.
	show running-config	Added the **interface**, **policy**, **snmp**, **virtual-blade**, and **wccp** options to limit the display of configuration information.
	show statistics accelerator http	Added the **debug** and **https** options to display debugging and HTTPS statistics.
	show statistics accelerator ssl	Added the **payload, https**, and **other** options to display payload type, HTTPS flow, and unidentified flow statistics.
	show statistics filtering	Added several new counters.
Global configuration	**accelerator http**	Added the **dre-hints**, **request-ignore-no-cache**, **response-ignore-no-cache**, and **https** options.
	tacacs	Added the **port** option to specify the TACACS+ server port.

Software Version 4.3.1 Monitoring API

This section includes the following topics:

- Software Version 4.3.1 Monitoring API Changes
- Using Previous Client Code

Software Version 4.3.1 Monitoring API Changes

Table 3 lists the new Monitoring APIs in WAAS version 4.3.1.

Table 3 New Monitoring APIs

Web Service	API Name
DeviceConf	getDevice
	getDevices
	getDeviceByName
	getDevicesInGroup
	getDevicesInGroupByName
	getDevicesPerLocation
HttpsStats (new service	getConnOptType
	retrieveResponseStats
	retrieveStats
TrafficStats	retrieveAverageThroughPutStats
	retrieveConnectionTrendStats
	retrievePeakThroughPutStats

Additionally, the following new web service objects are added: ConnectionTrendStats, AverageThroughPutStats, HttpsStats, HttpsConnOptType, HttpsResponseStats, and PeakThroughPutStats

Using Previous Client Code

If you have upgraded to WAAS version 4.3.1 and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code may return unexpected exceptions due to new elements added in the response structures in 4.3.1. The observed symptom is an exception related to an unexpected subelement because of the new element (for example, a deviceName element) in the XML response.

To work around this problem, we recommend that you patch the WSDL2Java tool library to silently consume exceptions if new elements are found in XML responses, then regenerate the client stubs. This approach avoids future problems if the API is enhanced with new elements over time.

You must modify the ADBBeanTemplate.xsl file in the axis2-adb-codegen-*version*.jar file.

To apply the patch, follow these steps:

Step 1 List the files in the axis2-adb-codegen-*version*.jar file:

```
#jar tf axis2-adb-codegen-1.3.jar

META-INF/
META-INF/MANIFEST.MF
org/
org/apache/
org/apache/axis2/
org/apache/axis2/schema/
org/apache/axis2/schema/i18n/
org/apache/axis2/schema/template/
org/apache/axis2/schema/typemap/
org/apache/axis2/schema/util/
org/apache/axis2/schema/writer/
```

```
org/apache/axis2/schema/i18n/resource.properties
org/apache/axis2/schema/i18n/SchemaCompilerMessages.class
org/apache/axis2/schema/template/ADBDatabindingTemplate.xsl
org/apache/axis2/schema/template/CADBBeanTemplateHeader.xsl
org/apache/axis2/schema/template/CADBBeanTemplateSource.xsl
org/apache/axis2/schema/template/PlainBeanTemplate.xsl
org/apache/axis2/schema/template/ADBBeanTemplate.xsl
org/apache/axis2/schema/c-schema-compile.properties
org/apache/axis2/schema/schema-compile.properties
org/apache/axis2/schema/typemap/JavaTypeMap.class
org/apache/axis2/schema/typemap/TypeMap.class
org/apache/axis2/schema/typemap/CTypeMap.class
org/apache/axis2/schema/util/PrimitiveTypeWrapper.class
org/apache/axis2/schema/util/PrimitiveTypeFinder.class
org/apache/axis2/schema/util/SchemaPropertyLoader.class
org/apache/axis2/schema/SchemaConstants$SchemaPropertyNames.class
org/apache/axis2/schema/SchemaConstants$SchemaCompilerArguments.class
org/apache/axis2/schema/SchemaConstants$SchemaCompilerInfoHolder.class
org/apache/axis2/schema/SchemaConstants.class
org/apache/axis2/schema/ExtensionUtility.class
org/apache/axis2/schema/CompilerOptions.class
org/apache/axis2/schema/writer/BeanWriter.class
org/apache/axis2/schema/writer/JavaBeanWriter.class
org/apache/axis2/schema/writer/CStructWriter.class
org/apache/axis2/schema/SchemaCompilationException.class
org/apache/axis2/schema/BeanWriterMetaInfoHolder.class
org/apache/axis2/schema/SchemaCompiler.class
org/apache/axis2/schema/XSD2Java.class
META-INF/maven/
META-INF/maven/org.apache.axis2/
META-INF/maven/org.apache.axis2/axis2-adb-codegen/
META-INF/maven/org.apache.axis2/axis2-adb-codegen/pom.xml
META-INF/maven/org.apache.axis2/axis2-adb-codegen/pom.properties
```

Step 2 Change the ADBBeanTemplate.xsl file by commenting out the following exceptions so that the generated code will consume the exceptions:

```
<xsl:if test="$ordered and $min!=0">
  else{
    // A start element we are not expecting indicates an invalid parameter was passed
    // throw new org.apache.axis2.databinding.ADBException("Unexpected subelement " +
reader.getLocalName());
  }
</xsl:if>

. . .

  while (!reader.isStartElement() &amp;amp;&amp;amp; !reader.isEndElement())
    reader.next();
  //if (reader.isStartElement())
    // A start element we are not expecting indicates a trailing invalid property
    // throw new org.apache.axis2.databinding.ADBException("Unexpected subelement " +
reader.getLocalName());
</xsl:if>

. . .

<xsl:if test="not(property/enumFacet)">
  else{
    // A start element we are not expecting indicates an invalid parameter was passed
    // throw new org.apache.axis2.databinding.ADBException("Unexpected subelement " +
reader.getLocalName());
  }
```

Step 3 Recreate the jar file and place it in the CLASSPATH. Delete the old jar file from the CLASSPATH.

Step 4 Use the WDL2Java tool to execute the client code using the modified jar.

WAAS Documentation Set

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

- *Cisco Wide Area Application Services Upgrade Guide*
- *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 Wide Area Application Services Monitoring Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Cisco Wide Area Application Services Online Help*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *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*
- *Installing the Cisco WAE Inline Network Adapter*

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.