Release Note for Cisco Wide Area Application Services Software Version 4.2.1

August 8, 2012

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

Contents

This release note applies to the Cisco Wide Area Application Services (WAAS) software version 4.2.1.

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

- WAAS Documentation Set
- Obtaining Documentation and Submitting a Service Request

New and Changed Features

The following section contains the following topics:

- Software Version 4.2.1 New and Changed Features
- Software Version 4.2.1 Deprecated Features
- Software Version 4.2.1 Filenames

Software Version 4.2.1 New and Changed Features

WAAS software version 4.2.1 includes the following new features and changes:

- SM/SRE support—WAAS now supports the SM-SRE-700 and SM-SRE-900 Services Ready Engine (SRE) Service Modules for Cisco Integrated Services Router Generation 2 (ISR G2).

  For SM/SRE modules, we recommend using Cisco IOS Software Release 15.0(1)M3, which is scheduled for release in July 2010. Until then, you may use Cisco IOS Software Release 15.0(1)M2, noting the following caveats: CSCtf17799, CSCtf40425, and CSCsy31597.

- HTTP accelerator enhancements—The HTTP accelerator in the branch WAE can cache particular server responses (HTTP responses 301, 304, and 401) and respond locally to clients. The HTTP accelerator can also suppress Accept-Encoding compress, gzip, and deflate request-headers between the client and the server, allowing the WAE to compress HTTP data instead of the server. Finally, the HTTP accelerator uses internal DRE hinting. All these changes improve the HTTP accelerator throughput and compression, and improve application response time. For more information, see the section "Configuring HTTP Acceleration" in Chapter 12, "Configuring Application Acceleration," in the *Cisco Wide Area Application Services Configuration Guide*.

- SSL accelerator enhancements—The SSL accelerator is enhanced to allow configuring accelerated services based on wildcard-matched domain names and hostnames, enabling easier deployment of the acceleration of cloud-based SaaS applications and enterprise SSL applications. This enhancement simplifies migration to cloud services while retaining the benefits of WAN optimization. Additionally, the Central Manager administrative service can now use custom certificates and keys. For more information, see the section "Configuring SSL Acceleration" in Chapter 12, "Configuring Application Acceleration," in the *Cisco Wide Area Application Services Configuration Guide*.

- Virtual blade enhancements—The virtualization feature is enhanced to support multiple CPUs, network install and boot capability (PXE) for guest operating systems, paravirtualized network drivers for higher performance, Windows Server 2008 R2 support, and other usability improvements. For more information, see Chapter 14, "Configuring Virtual Blades," in the *Cisco Wide Area Application Services Configuration Guide*.

- Serial Inline Clustering enhancements—The following enhancements improve the ability to serially cluster WAEs using inline interception mode, particularly in data centers:

  – Two Cisco WAE Inline Network Adapters are now supported in WAE-7341, WAE-7371, and WAE-674 models.

  – New configuration options allow you to configure the serial peer device to disable optimization between the serial peers.

  - A new interception ACL allows you to control traffic interception on a WAE device and bypass any non-relevant traffic with one ACL.

  For more information, see Chapter 4, "Configuring Traffic Interception," in the *Cisco Wide Area Application Services Configuration Guide*.

- Setup utility enhancement—The setup utility is enhanced to increase usability, give more control to users, provide more functionality, and support SM-SRE and NME-WAE WCCP configuration.
- MAPI accelerator enhancements—The MAPI accelerator is enhanced to improve stability and allow configuration of the maximum number of reserved connections.
- CIFS accelerator enhancements—The CIFS accelerator is enhanced to improve prepositioning scalability and stability.
- Command Authorization—This new feature allows all CLI commands to be authorized through an external TACACS+ server. For more information, see the section "Configuring AAA Command Authorization" in Chapter 6, "Configuring Administrative Login Authentication, Authorization, and Accounting," in the *Cisco Wide Area Application Services Configuration Guide*.
- Central Manager—The Central Manager is enhanced to improve usability, add location-based reporting, and includes numerous monitoring and reporting enhancements. Two fields, Reduction (%) Including Pass-Through and Effective Capacity Including Pass-Through, were removed from the Traffic Summary table to avoid mixing optimized and pass-through traffic statistics.
- Software image size reduced—The WAAS software image size is reduced by over 50 percent, enabling easier network distribution. Additionally, there is now an even smaller alternate software image that supports accelerator mode only.
- WCCP enhancements—The WCCP default mask is changed from 0x1741 to 0xF00 to provide better WAE load balancing and lower router TCAM usage in typical deployments. (Already configured WAE masks are not changed, only newly configured WAEs use the new default mask.) New alarms alert users to common problems with WCCP service groups. Additionally, WCCP control messages are now marked with a DSCP value of 192 (IPTOS_INTERNET_CONTROL) to prioritize them over other locally destined packets.
- SNMP enhancements—SNMP is enhanced to support two new traps to monitor link status.
- The XML API—The Central Manager XML API is enhanced to support location reporting and several new API functions are available to increase the type of information that can be retrieved.
- CLI commands—For CLI command changes, see the "Software Version 4.2.1 Command Changes" section on page 16.

Software Version 4.2.1 Deprecated Features

The following features are deprecated and no longer supported in WAAS software version 4.2.1:

- Legacy WAFS and Print Services—The legacy WAFS mode and legacy print services features are deprecated and no longer supported. These features continue to function in this release but are not supported. They will be removed in a future release.
- WAE-511/611—The WAE-511 and WAE-611 hardware platforms are no longer supported.

Software Version 4.2.1 Filenames

WAAS software version 4.2.1 includes the following primary software image files:

- WAAS-4.2.1.38-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-4.2.1.38-K9.AA.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. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator only image.
- SM-WAAS-4.2.1.38-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-4.2.1.38-rescue-cdrom-K9.iso—WAAS software recovery CD image.
- WAAS-4.2.1.38-K9.x86_64.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-274/474/574 and WAE-674/7341/7371 devices).
- WAAS-4.2.1.38-K9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- WAAS-4.2.1.38-K9.kdump.bin—Kdump analysis component that you can install and use with the Application Accelerator software image.
- WAAS-4.2.1.38-DOC.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.)

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
- Prepositioning Interoperability

WCCP Interoperability

Central Managers running version 4.2.1 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 4.2.1

To upgrade from WAAS prerelease software to version 4.2.1, 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 Version 4.0.x or 4.1.x to 4.2.1

This section contains the following topics:

- Requirements and Guidelines
- Ensuring a Successful RAID Pair Rebuild

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

Requirements and Guidelines

When you upgrade from version 4.0.x or 4.1.x to version 4.2.1, observe the following guidelines and requirements:

- Upgrading to version 4.2.1 is supported only from versions 4.0.19, 4.0.25, 4.0.27, 4.1.1d, 4.1.3, 4.1.3a, 4.1.3b, 4.1.5b, 4.1.5c, 4.1.5d, 4.1.5e, 4.1.5f, and 4.1.7. 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 4.2.1 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 4.2.1, 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 4.2.1x using the **Jobs > Software Update** page from a 4.0.x WAAS Central Manager, enter 4.2.1.0.1 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 Chapter 12, "Configuring Application Acceleration," in the *Cisco Wide Area Application Services Configuration Guide*.
- WAAS version 4.2.1 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 4.2.1 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 4.2.1, 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 4.2.1, 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 4.2.1, 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 4.2.1, 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 4.2.1, 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 4.2.1, 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 4.2.1, invalid settings in these fields are deleted.
- Central Manager support for configuring the Initial Slow Start Threshold TCP/IP setting is removed in version 4.2.1. If your Central Manager is managing devices lower 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 4.2.1, 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 4.1.x to version 4.2.1, and you have any scheduled reports that are configured for a very large number of recurrences (99,999 or more), before you upgrade you must delete such reports and reschedule them with a lower number of recurrences, otherwise, the Central Manager can become inaccessible after the upgrade.
- After upgrading a Central Manager from version 4.1.x to version 4.2.1, 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 4.2.1, any scheduled reports that are pending (not yet completed) are removed. To continue generating these reports, reschedule them.
- After upgrading a Central Manager to version 4.2.1, in the Jobs > Software Update page, any previously added software image files show an image type of Unknown. These Unknown software files must be resubmitted if you want to use them. Click the **Edit** icon next to the file to open the Modifying Software File window, then click the **Submit** button to resubmit the file.

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 4.2.1 to a Previous Version

Note the following guidelines for downgrading:

- Downgrade is supported only to versions 4.1.7, 4.1.5f, 4.1.5e, 4.1.5d, 4.1.5c, 4.1.5b, 4.1.3b, 4.1.3a, 4.1.3, 4.1.1d, 4.0.27, 4.0.25, or 4.0.19.
- 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.
- 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.
- Due to stricter security implemented in version 4.2.1, when downgrading from version 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 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**.
- 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 4.2.1 are removed from managed reports and scheduled reports when downgrading to a version prior to 4.2.1.

- The default value for the WCCP source IP mask changed in version 4.2.1 to 0xF00. If you are downgrading a 4.2.1 WAE that uses the default WCCP source IP mask, its WCCP mask is not changed on downgrade. Note that all WAEs in a WCCP service group must have the same mask.

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.1.7, 4.1.5f, 4.1.5e, 4.1.5d, 4.1.5c, 4.1.5b, 4.1.3b, 4.1.3a, 4.1.3, 4.1.1d, 4.0.27, 4.0.25, or 4.0.19, 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 4.2.1:

- Interoperability
- Virtual Blade Configuration From File
- Device Group Default Settings
- Using Autoregistration with Port-Channel Interfaces
- WAFS Support of FAT32 File Servers
- Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.2.1 devices with devices running earlier software versions.

- WAAS version 4.2.1 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 4.2.1. 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 4.2.1, the WAAS Central Manager must be running the highest version of the WAAS software.
- When a WAAS Central Manager is upgraded to version 4.2.1 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.

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 4.2.1, 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**

Software Version 4.2.1 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.2.1:

- Software Version 4.2.1 Resolved Caveats
- Software Version 4.2.1 Open Caveats
- Software Version 4.2.1 Command Changes
- Software Version 4.2.1 Monitoring API Changes

Software Version 4.2.1 Resolved Caveats

The following caveats were resolved in software version 4.2.1.

Caveat ID Number	Description
CSCsu04285	Passthrough reason shown as PT Rjct Resources when no license configured
CSCsu12114	LZ compression fails, with read only filesystem due to journal errors
CSCsw14753	Unable to remove a file without write permission
CSCsx61934	Access-list fails to block traffic when WCCP GRE is used.
CSCsx66071	Preposition task may be started randomly assuming a wrong time zone
CSCsx78566	Under rare conditions, cannot delete dynamic shares from the CM
CSCsy31216	Incorrect reference count is displayed after concurrent CIFS traffic
CSCsy99732	In rare cases duplicate emails or send failures may be seen
CSCsz74788	"sh stat conn opt" displays mismatched flow statistics
CSCta08640	Server may deny access to share via CIFS AO
CSCta15567	A core file has been created by mapi process during long duration test
CSCta27928	The ifLastChange value is not within the sysUpTime range.
CSCta32790	Data Server error seen while trying to enable SNMP traps
CSCta38419	Under rare conditions VB may crash when a RAID disk fails
CSCta85182	Unable to override policy settings on Re-registration of WAE.
CSCtb16690	Running config shows invalid secondary ip addresses for Inline
CSCtb18370	Name field in CM GUI may show wrong values when a device is inactivated
CSCtb27676	SMBFormatException seen in edge cifs error log in particular scenario
CSCtb28415	CIFS AO went to error state when running load test
CSCtb33749	CIFS AO keeaplive failures seen on WAE during non-CIFS traffic request
CSCtb33915	Device reboots after tethereal run for many hours for troubleshooting
CSCtb36731	WAE may try secondary server even after primary rejects authentication
CSCtb48871	WAAS 4.1.3 TFO runs slower than 4.0
CSCtb57441	WCCP corefile seen when new rtr in farm does not support assign method
CSCtb73175	Rarely emails sent incorrectly with Exchange 2007 under server load
CSCtb74241	In a rare case scenario HTTP connection may fail with inline mode
CSCtb85564	WAAS NTP authentication may not succeed in some cases
CSCtc13699	"FSClient OPEN failed with error" seen in cifs_err.log of DC WAE
CSCtc39508	WAVE configured as a standby group may lose connectivity after upgrade
CSCtd19677	In rare case, WAE-7326 power monitoring impacts performance
CSCtd42371	Communication between CM and WAE is broken after restoring CM db backup
CSCtd54221	Inline Interface goes to Bypass mode during long duration soak Test
CSCtd60131	Device reporting alarm "actastor_watchdog service has been disabled"
CSCte26428	SNMP commands added to Standby CM when WAE is registered.

Caveat ID Number	Description
CSCte43679	WAE goes offline , RMI fail and logs conn refused to local host msg
CSCte43688	"disk delete-data-partition" CLI help text states incomplete impact
CSCte46265	Error message spamming the log when win 7 client logs off
CSCtf60675	SMB flow may fail and exception seen with a custom app Cmacntrl
CSCtf70873	Offline: CIFS cache not getting updated after synchronization.

Software Version 4.2.1 Open Caveats

The following open caveats apply to software version 4.2.1.

Caveat ID Number	Description
CSCsj95489	Client throws error during Big file copy
CSCsr88316	WAFS Edge or CIFS-AO restarts due to false liveliness alarm
CSCsu65901	In a rare scenario, java corefile seen on a 274 WAE running HTTP traffic
CSCsv79472	Edge/Core restarts due to liveliness alarm
CSCsx06436	Under rare conditions, configuration made in CLI is overwritten by CM
CSCsx64796	CIFS AO may generate core on large print jobs while low on memory
CSCta05256	cifs liveliness error messages encountered-cifs servc dead alarms
CSCtb29132	Upgrade failure can happen in rare scenario
CSCtd70016	Under rare circumstances, after reload, CIFS AO can not be re-enabled
CSCte72709	CIFS/Print: stapling/duplex printing for Canon driver makes Conn fail
CSCte86102	Preposition root share may get deleted without user intervention
CSCte94652	SETUP on SM/SRE becomes unreadable while using command prompt
CSCte98452	CIFS: Samba clients talking to Samba server can't write or copy files
CSCtf03624	Big file copy may fail with vista client with cifsao
CSCtf31614	In rare case, CifsAO can cause a core file to be created
CSCtf87641	Rarely MAPI AO may restart causing Outlook to re-establish connections
CSCtf97106	CIFS acceleration reports graph may show value of '1' always
CSCtg19458	Rarely connection reset when copy large folder, Outlook 2k7 online mode.
CSCtg53099	Win7/Win2008 clients unable to access legacy print-srvces using hostname
CSCtg75659	WCCP page goes to override mode on upgrade in a specific scenario
CSCtg80555	Software download status continues to show 'Pending' in specific case
CSCtg86680	Diagnostic tool shows incorrect info on default gateway and CM
CSCtg86826	Windows 2003-R2 VB with old Intel e1000 driver unable to reach WAE IP
CSCth42086	Configuring wccp from setup-wizard can cause rtr_unreachabe alarm
CSCth86035	Double byte name of files/folders isn't cached properly in WAAS 4.2.1

Software Version 4.2.1 Command Changes

This section lists the new and modified commands in WAAS software version 4.2.1.

Table 1 lists the new commands and options that have been added in WAAS software version 4.2.1.

Table 1 CLI Commands Added in Version 4.2.1

Mode	Command	Description
EXEC	**debug aaa authorization**	Monitors and records command authorization debugging.
	show aaa authorization	Displays command authorization configuration information.
	show cache http-metadatacache	Displays HTTP metadata cache information.
	show device-id	Displays the WAAS device ID.
	show peer optimization	Displays the configured serial peers for a WAAS device.
	top	Displays the current top CPU processes.
Global configuration	**aaa authorization commands**	Configures command authorization.
	disk object-cache extend	Enables/disables the extended object cache.
	interception access-list	Configures an interception ACL.
	peer	Enables/disables peer optimization.
Virtual Blade configuration	**cpu-list**	Configures the CPU assignments that the virtual blade runs on.

Table 2 lists existing commands that have been modified in WAAS version 4.2.1.

Table 2 CLI Commands Modified in Version 4.2.1

Mode	Command	Description
EXEC	**clear cache dre**	Now asks if you want to save configuration changes if a reboot is required.
	clear cache http	Added the **http-metadatacache** option to clear the HTTP accelerator metadata cache.
	cms secure-store reset	Now works on devices in application-accelerator mode.
	crypto delete	Added new **admin** option.
	crypto export	Added new **admin** option.
	crypto import	Added new **admin** option.
	debug accelerator http	Added options to debug new HTTP accelerator features.
	show accelerator http	Added the **debug** option, which displays several counters for new HTTP accelerator features.
	show authentication	Added the **strict-password-policy** option, which displays strict password policy configuration information.
	show crypto	Added the **admin** option, which displays admin service certificate information, and the **ssl services** option, which displays the status of SSL services.
	show disk details	Added status of extended object cache feature.
	show hardware	Added display of device ID.
	show interface	Removed the **usb** option because it does not apply to WAAS devices.
	show ip access-list	Added display of interception ACLs.
	show kdump	Added display of kdump package installation status.
	show key-manager	Changed **key** option to **key-token** and enhanced output.
	show processes cpu	Added display of average and peak CPU usage.
	show statistics accelerator http detail	Added several counters for new HTTP accelerator features.
	show statistics accelerator mapi detail	Added several counters.

Table 2 CLI Commands Modified in Version 4.2.1 (continued)

Mode	Command	Description
	show statistics auto-discovery	Added new counter: Connections taken over for MAPI optimization.
	show statistics filtering	Added new counters: • SYN packets sent with non-opt option due to MAPI • Internal Server conn. not optimized due to Serial Peer
	show statistics pass-through	Added new counters: • Peer Override • Non-optimizing Peer • Interception ACL
	show version	Added display of the software image type.
	show virtual-blade	Added new **detail** option.
	virtual-blade	Added new **reset** option and behavior of **stop** option changed.
Global configuration	**accelerator http**	Added the **metadatacache** option to control HTTP metadatacaching and the **suppress-server-encoding** option to control suppression of server encoding.
	accelerator mapi	Added the **reserved-pool-size** option to configure the maximum reserved connection pool percent for MAPI acceleration.
	authentication strict-password-policy	Added the **max-retry-attempts** option to control the number of failed login attempts allowed before locking out the user.
	interface InlineGroup	Added the **ip** option to assign an IP ACL to an inline interface, and added the **cdp enable** option.
	logging console **logging disk** **logging host**	Added the ability to specify priority by numeric level.
	snmp-server enable traps	Added the **linkdown** and **linkup** options to the **snmp** option.
	snmp-server user	Changed **user** *name* maximum length to 32 characters. Changed **remote** *octetstring* minimum length to 10 characters and maximum length to 64 characters.
	tfo tcp adaptive-buffer-sizing **tfo tcp optimized-receive-buffer** **tfo tcp optimized-send-buffer** **tfo tcp original-receive-buffer** **tfo tcp original-send-buffer**	Changed maximum size of buffers to 32768 KB.
	username	The **no** option now allows you to remove the print admin privilege from a user.
	wccp tcp-promiscuous mask	Changed the default source IP address mask to 0xF00.

Table 2 CLI Commands Modified in Version 4.2.1 (continued)

Mode	Command	Description
Virtual Blade configuration	**boot**	Added the **network** option to boot from the network.

Table 3 lists commands that have been deprecated in WAAS version 4.2.1. These commands still work but are not supported and will be removed in a future software version.

Table 3 CLI Commands Deprecated in Version 4.2.1

Mode	Command	Description
Global configuration	**print-services**	Legacy print services are deprecated.
	smb-conf	Options that configure legacy print services are deprecated.
	username print-admin-password	Legacy print services are deprecated.

Software Version 4.2.1 Monitoring API Changes

Table 4 lists the new Monitoring APIs in WAAS software version 4.2.1:

Table 4 New APIs

Web Service	API Name	Input Parameters	Output Parameters
DeviceConf	getAPIVersion	none	String
	getLocations	none	Location
	getWAEsPerLocation	id:long	String[]
HttpStats	retrieveResponseStats	name:string objType:string timeframe:TimeFrameFilter	HttpResponseStats
	getConnOptType	name:string objType:string timeframe:TimeFrameFilter	HttpConnOptType
	getUnaccelConnCount	name:string objType:string timeframe:TimeFrameFilter	HttpUnaccelConnCount
MapiStats	getOptConnCount	name:string objType:string timeframe:TimeFrameFilter	MapiOptConnCount
	getUnaccelConnCount	name:string objType:string timeframe:TimeFrameFilter	MapiUnaccelConnCount
	getDroppedConnCount	name:string objType:string timeframe:TimeFrameFilter	MapiDroppedConnCount

Table 4 New APIs (continued)

Web Service	API Name	Input Parameters	Output Parameters
NfsStats	getOptConnCount	name:string objType:string timeframe:TimeFrameFilter	NfsOptConnCount
	getUnaccelConnCount	name:string objType:string timeframe:TimeFrameFilter	NfsUnaccelConnCount
	getDroppedConnCount	name:string objType:string timeframe:TimeFrameFilter	NfsDroppedConnCount
SslStats	getActiveConnCount	name:string objType:string timeframe:TimeFrameFilter	SSLActiveConnCount
VideoStats	getActiveConnCount	name:string objType:string timeframe:TimeFrameFilter	VideoActiveConnCount
	getAccelerationBypassReasons	name:string objType:string timeframe:TimeFrameFilter	VideoAccelBypassReasons

Additionally, note these other Monitoring API changes:

- A new frequency of last5min is added to the TimeFrameFilter object.
- A new deviceName value is added to the TrafficStats object.
- A new Location object is added for retrieving location based statistics.

Upgrading with Monitoring API Using WSDL2Java Client

If you have upgraded to WAAS version 4.2.1 and are using the WSDL2Java tool to generate client stubs that enforce strict binding, version 4.1.x client code may return unexpected exceptions due to new elements added in the response structures in 4.2.1. 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 enables 4.1.x WSDL2Java clients to continue to use 4.2.1 monitoring APIs and APIs that may have additional elements in future releases.

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; !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 regenerate the client stub 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 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.