Release Note for Cisco Wide Area Application Services Software Version 4.4.1x

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:

- 4.4.1

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:

- New and Changed Features
- Upgrading from WAFS to WAAS
- Upgrading and Interoperability
- Upgrading from a Prerelease Version to Version 4.4.1
- Upgrading from a Release Version to Version 4.4.1
- Downgrading from Version 4.4.1 to a Previous Version
- Cisco WAE and WAVE Appliance Boot Process
- Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade
- Cisco WAE-612 Hard Disk Drive Replacement Notification

Cisco Systems, Inc.
www.cisco.com

- Operating Considerations
- Software Version 4.4.1 Resolved Caveats, Open Caveats, and Command Changes
- WAAS Documentation Set
- Obtaining Documentation and Submitting a Service Request

New and Changed Features

The following section contains the new and changed features in software version 4.4.1:

- Software Version 4.4.1 New and Changed Features
- Software Version 4.4.1 Filenames

Software Version 4.4.1 New and Changed Features

WAAS software version 4.4.1 includes the following new features and changes:

- Support for six new WAAS appliances—The WAVE-294, WAVE-594, WAVE-694, WAVE-7541, WAVE-7571, and WAVE-8541 WAAS appliances are introduced and supported. Additionally, this release supports the following four new interchangeable interface modules that are used in the new appliances: 4xGE copper, 8xGE copper, 4xGE fiber, 2x10GE fiber (supported only on WAVE-75xx and WAVE-85xx appliances). Most of these interface modules can be configured to operate either with WCCP or inline interception.
- Application Aware DRE—The Data Redundancy Elimination (DRE) feature is enhanced to allow unidirectional caching in addition to bidirectional caching. This feature together with other internal enhancements significantly improves DRE performance and caching efficiency for many applications. You also can configure DRE to adapt dynamically and use the best caching mode based on the application traffic characteristics.
- Integrated Application Performance Monitoring—Application performance monitoring capabilities are enhanced by integrating access to the Cisco Network Analysis Module (NAM) Traffic Analyzer into the Central Manager. If your network includes a NAM 5.1 server (physical or virtual), you can access NAM configuration and reporting tasks from within the WAAS Central Manager. Key performance metrics such as application response time before and after WAN optimization, top talkers, network throughput, and usage baseline are available from the Central Manager.
- HTTP Application Acceleration Enhancement—The HTTP application accelerator is enhanced to support subnets, which can be configured to selectively disable or enable specific HTTP acceleration features for specific groups of clients. This gives you more control over what HTTP optimizations are applied to specific connections.
- WCCP enhancements—Enhancements include configurable WCCP service IDs and a variable failure detection timeout period. These enhancements allow routers to support multiple WAAS WCCP farms and to more quickly detect and respond to WAAS device failures (if the router also supports variable failure detection timeouts). Additionally, the WCCP load balancing assignment method is now always strictly enforced and must match the farm assignment method or the WAAS device is not allowed to join the farm.
- Secure Store enhancements—The Central Manager secure store can be configured in an automatic passphrase mode, which avoids the necessity to manually reopen the secure store following a system reboot. This also avoids having to reset the secure store if the password is lost because the password is automatically generated and then supplied by the Central Manager.

- Virtual Blades—Virtual interface configuration is enhanced to provide more flexibility through the use of Bridge Virtual Interfaces (BVI) and bridge groups that associate virtual blade interfaces to physical interfaces. Bridge groups can now use standby interfaces.
- SNMP—The new CISCO-WAN-OPTIMIZATION-MIB provides status and statistics for the application accelerators and TFO statistics.
- Legacy WAFS—Legacy WAFS support is removed. Users must use the transparent CIFS accelerator to accelerate file services.
- Legacy Print Services—Legacy print services support is removed. Users must use the Windows Print accelerator or a virtual blade based print server to accelerate network printing.
- WAE-511, WAE-611, and WAE-7326 platforms—These WAE models are no longer supported and WAAS version 4.4 does not operate on these appliances.
- CLI commands—For CLI command changes, see the "Software Version 4.4.1 Command Changes" section on page 18.
- Monitoring API—For API changes, see the "Software Version 4.4.1 Monitoring API" section on page 20.

Software Version 4.4.1 Filenames

WAAS software version 4.4.1 includes the following software image files for use on WAAS appliances and modules:

- Standard Image Files
- No Payload Encryption (NPE) Image Files

Standard Image Files

WAAS software version 4.4.1 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-4.4.1.*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-4.4.1.*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-4.4.1.*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-4.4.1.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-4.4.1.*x*-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-274/294/474/574/594/694/7541/7571/8541 and WAE-674/7341/7371 devices).
- waas-4.4.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).

- waas-kdump-4.4.1.*x*-k9.bin—Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following instructions by Cisco TAC.
- waas-alarm-error-books-4.4.1.*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 4.4.1 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-4.4.1.*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-4.4.1.*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-4.4.1.*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-4.4.1.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-4.4.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-274/294/474/574/594/694/7541/7571/8541 and WAE-674/7341/7371 devices).
- waas-4.4.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.4.1.*x*-npe-k9.bin—NPE Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following instructions by Cisco TAC.
- waas-alarm-error-books-4.4.1.*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

WAFS to WAAS version 4.4.1 (or later) migration is not supported. You must first migrate to a WAAS version prior to version 4.4.1, then upgrade to version 4.4.1 or later and migrate from the legacy WAFS mode to the transparent CIFS accelerator.

Upgrading and Interoperability

This section contains the following topics:

- WCCP Interoperability
- Prepositioning Interoperability

WCCP Interoperability

Central Managers running version 4.4.1 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 4.4.1

To upgrade from WAAS prerelease software to version 4.4.1, 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 4.4.1

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 to version 4.4.1, observe the following guidelines and requirements:

- Upgrading to version 4.4.1 is supported only from versions 4.1.1d, 4.1.3, 4.1.3b, 4.1.5c, 4.1.5f, 4.1.7, 4.1.7b, 4.2.1, 4.2.3, 4.2.3c, 4.3.1, 4.3.3, and 4.3.5. 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 4.4.1 version.
- Upgrading to version 4.4.1 is not supported on the following platforms: WAE-511, WAE-611, and WAE-7326. WAAS version 4.4.1 does not operate on these appliances.
- 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 4.4.1, 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.
- 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 CIFS 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*.
- If you are upgrading a WAAS Central Manager and have the secure store enabled, you must 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. After upgrading to version 4.4.1, you can change to auto-generated passphrase mode and you will no longer need to manually open the secure store after each reload. For more information on using the secure store, see the "Configuring Secure Store Settings" section in the *Cisco Wide Area Application Services Configuration Guide*.
- 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 4.4.1, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords and CIFS file server passwords. If you do not reenter the passwords, after upgrading to version 4.4.1, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- 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 4.2.3x or earlier to version 4.4.1, and you have any scheduled reports that are configured for more than 100 recurrences, after the upgrade only 100 recurrences are retained.
- If you use the setup utility for basic configuration after upgrading to 4.4.1, 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 is replaced with the new configuration.
- If you have disk encryption enabled and are upgrading to version 4.4.1 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 4.4.1 (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 from version 4.2.3x or earlier, the AllDevicesGroup device group is renamed to the AllWAASGroup. Additionally, an AllWAASExpressGroup is created for all WAAS Express devices.
- In version 4.4.1, application aware DRE changes the way the DRE cache is populated and managed. When upgrading to version 4.4.1 from version 4.3.x or earlier, the existing DRE cache is preserved, but all new cache entries are written in a new cache format. The two formats coexist until the old cache is evicted through the normal eviction processes.

  Application policies do not change, but the new “bidirectional” term is introduced, which is the mode used prior to version 4.4.1.

  DRE on a version 4.4.1 device is compatible with all version 4.1.x, 4.2.x, and 4.3.x peers, but is not compatible with 4.0.x peers.
- After upgrading WAE devices to version 4.4.1, you may be able to improve DRE disk performance by deleting and recreating disk data partitions by using the **disk delete-data-partitions** EXEC command. This command deletes the DRE and CIFS caches and all installed virtual blade images. If you want to keep virtual blade images, back them up before using this command by using the **copy virtual-blade** EXEC command.

  After using the **disk delete-data-partitions** command, you must reload the device and the data partitions are automatically recreated and the caches are initialized, which can take several minutes. DRE optimization is not done until the DRE cache has finished initializing. The **show statistics dre** EXEC command reports “TFO: Initializing disk cache” until then.
- After upgrading a Central Manager to version 4.4.1 from version 4.3.x or earlier, the secure store may be in one of two states:
  - If the secure store was previously initialized, the secure store is in user-passphrase mode and is not open. You must manually open it by supplying the passphrase.
  - If the secure store was previously uninitialized, the secure store is in auto-passphrase mode and is open. After a reboot, no user intervention is required to open the secure store.
- When upgrading a device to version 4.4.1, the WCCP load balancing assignment method is always strictly enforced and must match the farm assignment method or the WAAS device is not allowed to join the farm. Nonstrict assignment method is no longer an option.

When upgrading a Central Manager to version 4.4.1, the Only Use Selected Assignment Method check box is no longer available in the device group WCCP Settings window. Any WAEs in a device group that are running a version earlier than 4.4.1 and getting their WCCP settings from the device group will not use strict assignment method enforcement. This does not affect the WCCP farm.

- The method for associating virtual blade interfaces to physical interfaces changed in version 4.4.1 to use bridge groups and Bridge Virtual Interfaces (BVIs). When upgrading a device with a virtual blade to version 4.4.1, any virtual interface configurations are converted to use the new bridging method.
- Legacy mode WAFS is no longer supported in version 4.4.1 and upgrading to version 4.4.1 is prevented if legacy mode WAFS is enabled (edge or core services). Legacy WAFS users must migrate to the transparent CIFS accelerator before upgrading. For details on CIFS migration, see the *Cisco Wide Area Application Services Upgrade Guide*.
- Legacy mode print services is no longer supported in version 4.4.1. On upgrade to version 4.4.1, legacy print services functionality is removed and users must use the Windows Print accelerator. The print role and print admin privileges are removed from all user accounts, and the functionality of the Central Manager acting as a print repository is removed. Any legacy print services jobs that are spooled are lost if an upgrade to version 4.4.1 is done before the data is printed.

  A version 4.4.1 Central Manager can continue to manage earlier version WAEs that have legacy print services enabled, but print services can be configured on these WAEs only through the device CLI. The Central Manager also can display print services alarms from earlier version WAEs that are running legacy print services.

Upgrading From Version 4.1.x

The following guidelines and requirements apply only if you are upgrading from version 4.1.x:

- WAAS version 4.4.1 supports SSL application definition, which is enabled for monitoring by default. However, if you are upgrading from version 4.1.1 to version 4.4.1 and already have 20 applications enabled for monitoring, the new SSL application has 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.
- 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 4.1.1, other characters were allowed.) If you upgrade from version 4.1.1 to version 4.4.1, 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, only the group with the lowest priority and a valid member interface remains after the upgrade and it becomes standby interface 1. If the errors option was configured, it is removed.
- 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 4.4.1, 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 4.4.1, 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, 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.
- If you are upgrading a Central Manager from version 4.1.1x to version 4.4.1, 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.
- After upgrading a Central Manager from version 4.1.1x to version 4.4.1, any scheduled reports that are pending (not yet completed) will fail. To continue generating these reports, reschedule them.
- After upgrading a Central Manager from version 4.1.x to version 4.4.1, 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.
- The default value for the WCCP source IP mask changed in version 4.2.1 to 0xF00. If you are upgrading a version 4.1.x 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 4.1.x and earlier, 64 characters were allowed.) SNMP remote entity IDs must be between 10-32 hexadecimal characters. (In version 4.1.x and earlier, 1-64 characters were allowed.) If you upgrade from version 4.1.x or earlier to version 4.4.1, invalid settings in these fields are deleted.

Ensuring a Successful RAID Pair Rebuild

RAID pairs 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 4.4.1 to a Previous Version

Note the following guidelines and considerations for downgrading:

- Downgrade is supported only to versions 4.3.3, 4.3.1, 4.2.3c, 4.2.3, 4.2.1, 4.1.7b, 4.1.7, 4.1.5f, 4.1.5c, 4.1.3b, 4.1.3, and 4.1.1d. Downgrade is not supported to version 4.0.x.
- On a vWAAS device you cannot downgrade to a version earlier than 4.3.1.
- On WAVE-294/594/694/7541/7571/8541 models you cannot downgrade to a version earlier than 4.4.1.
- 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 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 must 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 are reset upon a downgrade.
- 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 4.4.1 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 4.4.1 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 is 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.
- When downgrading to a version earlier than 4.4.1, the DRE cache is cleared and the DRE caching mode for all application policies is changed to bidirectional (the only available mode prior to 4.4.1). Before downgrading a WAE, we recommend that you use the Central Manager GUI to change all policies that are using the new Unidirectional or Adaptive caching modes to the Bidirectional caching mode.
- When downgrading a Central Manager to a version earlier than 4.4.1, if the secure store is in auto-passphrase mode, downgrade is not allowed. You must switch to user-passphrase mode before you can downgrade to a software version that does not support auto-passphrase mode.
- Prior to downgrading to a version earlier than 4.4.1, we recommend that you change the WCCP service IDs back to their default values of 61 and 62, and change the failure detection timeout back to the default value of 30 seconds, if you have changed these values. Only these default values are supported in versions prior to 4.4.1 and any other values are lost after the downgrade. If a WAE is registered to a Central Manager, it is configured with the default service IDs of 61 and 62 after it is downgraded and comes back online.

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

Step 1 (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 2 Install the downgrade WAAS software image by using the **copy ftp install** EXEC command.

Step 3 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) or later 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_*xxxxx*_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware in the file named L4_*xxxxx*_FIRMWARE.pdf, which you can see when you mouse over the firmware file.

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 4.4.1:

- Interoperability
- Central Manager Report Scheduling
- WAAS Express Policy Changes
- Virtual Blade Configuration From File
- Device Group Default Settings
- Using Autoregistration with Port-Channel, Standby, and BVI Interfaces
- CIFS Support of FAT32 File Servers
- Microsoft Hotfix with CIFS
- Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP
- Disabling WCCP from the Central Manager
- Internet Explorer Certificate Request

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.4.1 devices with devices running earlier software versions.

- WAAS version 4.4.1 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 4.4.1. 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 4.4.1, the WAAS Central Manager must be running the highest version of the WAAS software.

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 lose all data on the virtual blade disks.

Device Group Default Settings

When you create a device group in WAAS version 4.4.1, 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, Standby, and BVI Interfaces

Autoregistration is designed to operate on the first network interface and will not work if this interface is part of a port-channel, standby, or bridge virtual interface (BVI). Do not enable the **auto-register** global configuration command when the interface is configured as part of a port-channel, standby, or BVI interface.

CIFS Support of FAT32 File Servers

The CIFS accelerator does not support file servers that use the FAT32 file system. You can use the policy engine rules to exclude from CIFS acceleration any file servers that use the FAT32 file system.

Microsoft Hotfix with CIFS

In deployments using the CIFS accelerator, we recommend installing Microsoft Hotfix 2434932 on client PCs using Microsoft Windows 7 or Windows Server 2008 R2. See http://support.microsoft.com/kb/2434932 for more information.

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**

Disabling WCCP from the Central Manager

If you use the Central Manager to disable WCCP on a WAAS device, the Central Manager immediately shuts down WCCP and closes any existing connections, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command. If you want to gracefully shut down WCCP connections, use the **no wccp version 2** global configuration command on the WAAS device.

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 4.4.1 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.4.1:

- Software Version 4.4.1 Resolved Caveats
- Software Version 4.4.1 Open Caveats
- Software Version 4.4.1 Command Changes
- Software Version 4.4.1 Monitoring API

Software Version 4.4.1 Resolved Caveats

The following caveats were resolved in software version 4.4.1.

Caveat ID Number	Description
CSCsu65901	In a rare scenario, java corefile seen on a 274 WAE running HTTP traffic
CSCtb79927	If CM device mode is config via setup wizard, reload should be requested
CSCtd78714	Disabling WCCP from CM causes few commands reconfig upon submit
CSCte66031	CSV export does not quote comma in the field
CSCth13281	Error messages in CIFS AO logs when there are too many connections
CSCth67290	Monitoring API - filter does not work for retrieveConnection API
CSCti93537	Sometimes TACACS+ packets contain DNS name in the "Remote Address" field
CSCtj05494	Running config doesnot reflect windows print accelerator CLI disable
CSCtj05828	Security updates to Apache Server code used in WAAS
CSCtj43510	MAPI AO may create core dump under rare circumstances of disconnects
CSCtj72402	On vWAAS with vPATH interception and mixed AO traffic, SSLAO restarted
CSCtk32205	RADIUS login fails when server response is larger than 1024 bytes
CSCtk57987	CIFS AO can restart when optimize servers that require digital signing
CSCtk76691	Watchdog alarm after WAE reboot because of corrupted config files
CSCtk83511	WAAS should passthrough traffic if device is degraded due to some reason
CSCtk84360	CIFS clients work slow via CIFS AO when there are too many connections

Caveat ID Number	Description
CSCtl03563	SNMP coredump seen on WAE devices when doing a memory free()
CSCtl09528	With a unique traffic pattern, the HTTP AO consumed a lot of memory
CSCtl11243	Unable to access shares via CIFS AO when there are too many connections
CSCtl17905	WAAS should operate with single disk if one disk fails on a RAID1 system
CSCtl43665	In device GUI, timeframe can not be set as year 2011 or later.
CSCtl44831	In a rare scenario, internal connection setup may result in box reboot
CSCtl71474	SNMP memory leak on query of ifTable causes service to restart
CSCtl74536	In rare case CIFS AO may misinterpret and cache a negative response
CSCtl77812	Pass through pkts drop in incorrect flow-protection state (IN w/o AWAY)
CSCtl89789	Several parallel SNMP get or show ops may trigger an internal error msg
CSCtn03341	TACACS+ key of length 32 or more characters is lost after reload
CSCtn05613	GUI statistics reports no or low data reduction
CSCto03691	Central Manager may fail to process cipher list updates from WAE
CSCto05106	Content of folder on S/390 V2R8M0 server not shown with CIFS AO enabled
CSCto13843	EPM: Errors seen while processing DPM traffic over DCOM protocol
CSCto42349	Some CIFS AO expert-mode configuration is not persistent
CSCto67614	'Getting null stats from device' warning may repeat in CM logs
CSCto74904	TACACS+ authentication fails due to timeout

Software Version 4.4.1 Open Caveats

The following open caveats apply to software version 4.4.1.

Caveat ID Number	Description
CSCsj95489	Can't copy file with additional data streams via CIFS AO
CSCsv79472	CIFS AO may restart due to liveliness alarm
CSCsx63833	In certain cases of segmentation fault, a core file was not created
CSCtd35001	Data sent by server dropped when FIN immediately follows http request
CSCtd70016	Under rare circumstances, CIFS AO can not be re-enabled
CSCtg87591	In certain RAID failures, an Invalid Controller Number is indicated.
CSCth44532	Outlook2K10 conns are not mapi optimized if profile contains > 1 account
CSCth83562	Video with stream number greater than 32 is not played through Video AO
CSCti20838	Modification of interface ACL via CM caused traffic drop
CSCtj00911	In rare cases, DRE hints stat may be incorrect when SSLAO is overloaded
CSCtk74707	Wrong Time under Connection Monitoring for WAE in CM
CSCtl88908	MAPI_AO restart under rare condition and created core
CSCtn11831	Printing via CIFS AO can be delayed when 64 bit server used

Caveat ID Number	Description
CSCtn31868	nscd service dead alarm raised and cleared in WAE periodically
CSCtn37732	show alarm reports incorrect disk# upon disk error during RAID rebuild
CSCtn65295	Can't access file on AS/400 V4R2 Server via CIFS AO
CSCtn96978	Rarely, false positive "wccp router unreachable" alarm may be seen on CM
CSCto12452	WAAS EPM traffic may be dropped by certain firewalls
CSCto62419	Accounting info from WAE on ACS 5.1 displays privilege 0 for Superuser
CSCto74161	Watchdog alarm may be reported after WAE reboot
CSCto88400	In rare cases, box may become unresponsive following clock change
CSCtq09096	Under certain conditions, schedule report e-mail may fail.
CSCtq21416	Under certain conditions, reports scheduled in 41x, 42x may fail.
CSCtq29244	Port Channel loses connectivity in a specific case when WAE intf is shut
CSCtq35903	Printer driver install via Print AO can fail(async DCERPC caching issue)
CSCtq47417	Alarm generated for CIFS AO down with misconfig Primary Interface
CSCtq52018	Policy classifier named as "All" may lead to inconsistent database in CM
CSCtq54882	Preposition task may work incorrectly if eth0,eth1,fa0,fa1 are down
CSCtw58778	WAVE694 raised alarm for missing PSU

Software Version 4.4.1 Command Changes

This section lists the new and modified commands in WAAS software version 4.4.1.

Table 1 lists the commands and options that have been added in WAAS version 4.4.1.

Table 1 CLI Commands Added in Version 4.4.1

Mode	Command	Description
EXEC	**copy usb**	Copies files from a USB storage device.
	clear bmc event-log	Clears the BMC event log.
	lsusb	Lists files or subdirectory names within a directory on a USB storage device.
	show bmc	Displays the Baseboard Management Controller (BMC) system event log.
Global configuration	**bridge**	Creates a bridge interface for use by a virtual blade.
	inline	Configures all ports on an interface module as inline interfaces.
	interface bvi	Configures a bridge virtual interface for a virtual blade.
	interface TenGigabitEthernet	Configures a 10 Gigabit Ethernet interface.
	wccp tcp-promiscuous service-pair	Configures WCCP service IDs and failure detection timeout.

Table 2 lists existing commands that have been modified in WAAS version 4.4.1.

Table 2 CLI Commands Modified in Version 4.4.1

Mode	Command	Description
EXEC	**clear arp-cache**	Added the **bvi**, **InlineGroup**, and **TenGigabitEthernet** options for new WAVE appliances.
	clear cache dre	No longer deletes the DRE cache contents but removes markers in the content to prevent reuse. If you want to delete the cache contents, use the **disk delete-data-partitions** command.
	cms secure-store	Added **mode** keyword and changed the way the secure store and existing keywords operate.
	copy ftp install	Added the **bios**, **bmc**, and **image** keywords.
	debug accelerator http	Added **subnet** keyword.
	install	Added the **bios** and **bmc** keywords.
	show accelerator http	Added output fields related to subnet feature.
	show cdp	Added the **TenGigabitEthernet** option to the **interface** and **neighbors** options for new WAVE appliances.
	show disks	Added the **fwlogs** option to the **tech-support** option for new WAVE appliances.
	show flash	Changed the output for new WAVE appliances.
	show hardware	Added support for 10 Gigabit Ethernet interfaces and other information on new WAVE appliances.
	show interface	Added the **bvi** and **TenGigabitEthernet** options.
	show inventory	Added information for Cisco Interface Modules, if installed.
	show statistics accelerator http	Added output fields related to subnet feature.
	show statistics connection	Changed output for **detail** option.
	show statistics dre	Changed output.
	show statistics peer dre detail	Changed output.
	show wccp	Added **details** option to **routers** keyword. Changed output for **services detail** and **routers** options.
	tcpdump	Can use WAAS port names to identify interfaces.
	tethereal	Can use WAAS port names to identify interfaces.
Global configuration	**accelerator http**	Added the **access-list** option to provide ACL control of individual HTTP accelerator features.
	auto-register	Added the **TenGigabitEthernet** option for new WAVE appliances.
	disk object-cache extend	Added support for the WAVE-694 appliance.
	interface gigabitethernet	Added the **bridge-group** option.
	interface portchannel	Added the **bridge-group** option and allowed configuration of up to four port channels on new WAVE appliances.
	interface standby	Added the **bridge-group** option and allowed configuration of up to two standby groups on new WAVE appliances.

Table 2 CLI Commands Modified in Version 4.4.1 (continued)

Mode	Command	Description
	policy-engine application map adaptor EPM	Added the **bidirectional**, **unidirectional**, and **adaptive** keywords.
	policy-engine application map basic	Added the **bidirectional**, **unidirectional**, and **adaptive** keywords.
	policy-engine application map other optimize DRE	Added the **bidirectional**, **unidirectional**, and **adaptive** keywords.
	primary-interface	Added the **TenGigabitEthernet** and **BVI** options and removed the **inlineGroup** option for new WAVE appliances.
	snmp-server trap-source	Added the **TenGigabitEthernet** option for new WAVE appliances.
	sshd	Maximum password guesses limited to three.
	tacacs	Limits key length to 32 characters maximum.
	wccp tcp-promiscuous router-list-num	Removed the **assign-method-strict** keyword (assignment method is now always enforced strictly).
Virtual blade configuration	**interface**	Added the **bridge-group** option for bridging to a bridge virtual interface. Removed the **bridge** option.

Table 3 lists the commands and options that have been removed in WAAS version 4.4.1.

Table 3 CLI Commands Removed in Version 4.4.1

Mode	Command	Description
EXEC	**debug authentication content-request**	Removed the **content-request** option because legacy WAFS mode is no longer supported.
	show authentication content-request	Removed the **content-request** option because legacy WAFS mode is no longer supported.
Global configuration	**authentication content-request**	Removed the **content-request** option because legacy WAFS mode is no longer supported.
	policy-engine application map adaptor WAFS transport	Removed the **WAFS transport** option because legacy WAFS mode is no longer supported.

Software Version 4.4.1 Monitoring API

This section includes the following topics:

- Software Version 4.4.1 Monitoring API Changes
- Using Previous Client Code

Software Version 4.4.1 Monitoring API Changes

Table 4 lists the modified Monitoring APIs in WAAS version 4.4.1. These changes are backwards compatible with existing code that uses the monitoring API.

Table 4 Modified Monitoring APIs

Web Service	API Name	Description
TrafficStats	retrieveConnection	The ConnectionStats returned object is enhanced with two new attributes: • classifier—The classifier applied to the connection, represented by a string value. • startTime—The connection start time, represented as a calendar object conforming to the XML dateTime schema specification.
TrafficStats	retrieveConnectionStats	The TrafficStats returned object is enhanced with two new attributes: • passthroughotherin—A long value that describes the incoming pass through traffic that is received from sources other than intermediate, policy, or peer traffic. • passthroughotherout—A long value that describes the outgoing pass through traffic that is received from sources other than intermediate, policy, or peer traffic.

Using Previous Client Code

If you have upgraded to WAAS version 4.4.1 and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code (prior to 4.3.1) may return unexpected exceptions due to new elements added in the response structures in 4.3.1 and later releases. 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 consumes 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 Wide Area Application Services vWAAS Installation and Configuration 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 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *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 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.