Release Note for Cisco Wide Area Application Services Software Version 4.5.1

March 11, 2015

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

Contents

These release notes apply to software Version 4.5.1 for the Cisco Wide Area Application Services (WAAS) software.

Note WAAS Release 4.5.1 is a limited availability release and is fully supported by the Cisco Technical Assistance Center (TAC) but is no longer available for customer testing or deployment. Customers who are currently running WAAS Release 4.5.1 should upgrade to newer versions, and new deployments should use newer versions that are fully released for general availability.

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 upgrading any other devices.

These release notes contain the following sections:

Cisco Systems, Inc.
www.cisco.com

New and Changed Features

The following section contains the new and changed features in software Version 4.5.1:

Software Version 4.5.1 New and Changed Features

WAAS software Version 4.5.1 includes the following new features and changes:

- ICA Application Acceleration—Supports WAN optimization of ICA (Independent Computing Architecture) traffic used to access a virtual desktop infrastructure (VDI). For more information, see the "ICA Application Acceleration" section.
- CLI commands—For CLI command changes, see the "Software Version 4.5.1 Resolved Caveats, Open Caveats, and Command Changes" section.

ICA Application Acceleration

ICA application acceleration provides WAN optimization on a WAAS device for ICA traffic to a VDI. This is done through a process that is both automatic and transparent to the client and server.

This section contains the following topics:

Note Citrix Multi-Stream ICA in XenDesktop 5.5 and XenApp 6.5 is not supported for optimization with WAAS 4.5.1.

Enabling ICA Acceleration

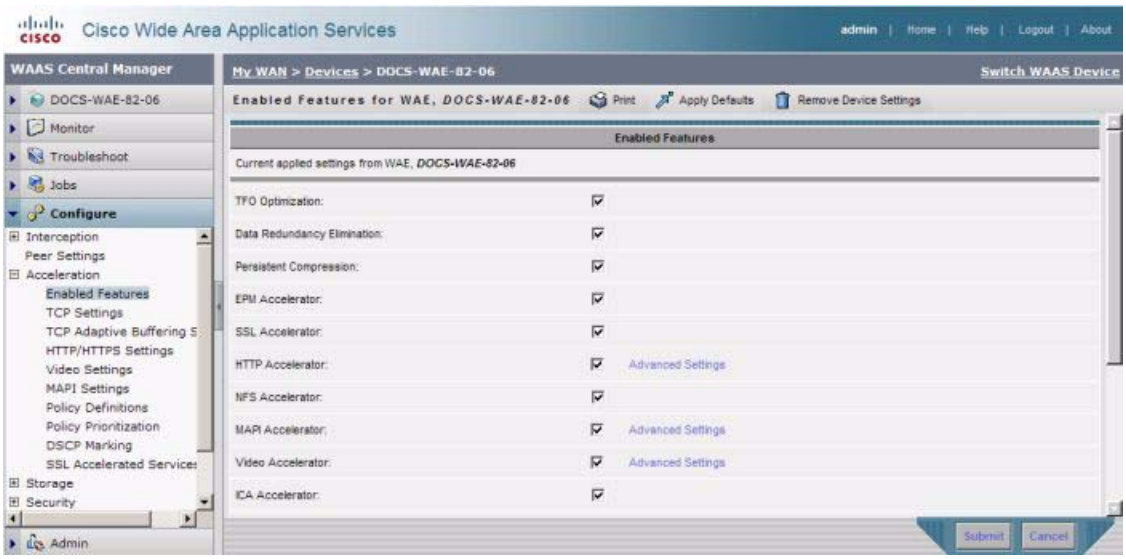
ICA acceleration is enabled on a WAAS device by default. If it has been disabled, follow these steps to enable ICA acceleration:

Step 1 From the WAAS Central Manager GUI, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to enable ICA acceleration.

Step 3 From the navigation pane, choose **Configure > Acceleration > Enabled Features**. The Enabled Features window appears. (See Figure 1.)

Figure 1 Enabled Features Window—ICA Acceleration



Step 4 Check the **ICA Accelerator** check box.

Note ICA acceleration is enabled by default.

Step 5 Click **Submit**.

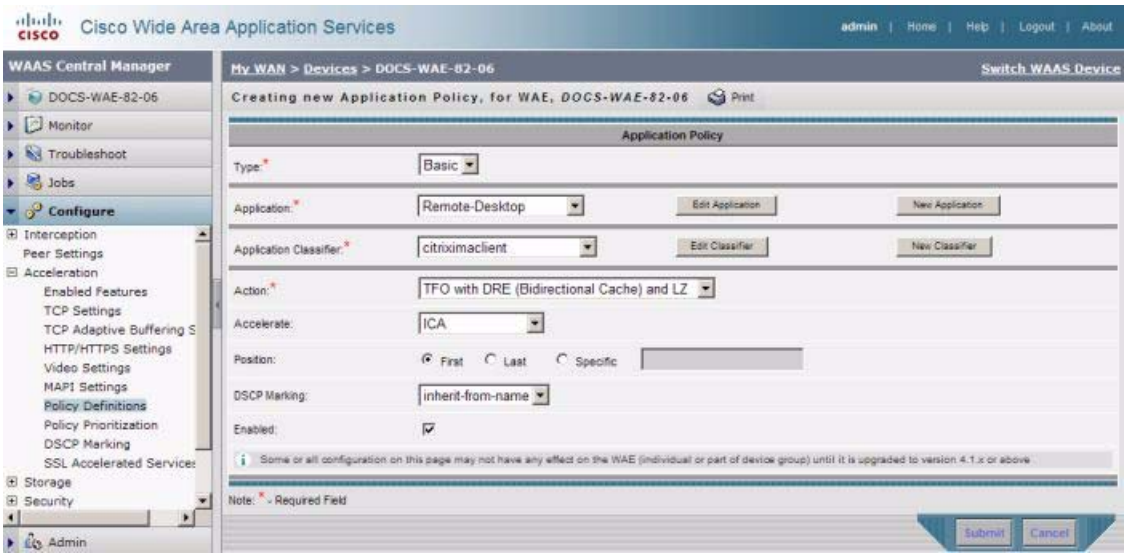
ICA Application Policy

The following changes have been made to the Application Policy window to support ICA optimization (See Figure 2.):

- Accelerate option: ICA
- Classifier options: ica, citriximaclient

See the *Cisco Wide Area Application Services Configuration Guide* for more information on application policy configuration.

Figure 2 Application Policy Window—ICA Acceleration



ICA Acceleration Reports

An ICA **Accelerator Report** option has been added to the Monitoring section of the WAAS Central Manager, including the following four charts:

- ICA Compression Over Time
- ICA Bandwidth Optimization
- ICA Optimized Traffic over Time
- ICA Optimized Connections over Time

All charts are based on TCP statistics but filtered on Remote-Desktop application. All charts are supported at the device, system, and location level, except the ICA Optimized Connections over Time chart, which is supported only at the device level.

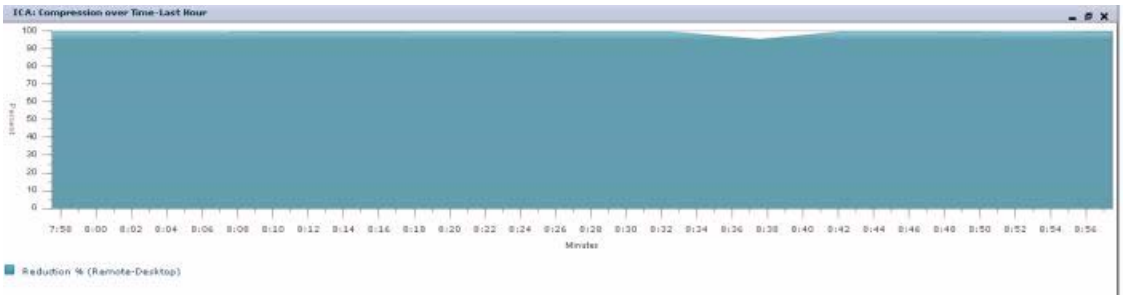
If the Remote-Desktop application is not created or has been renamed on the Central Manager, you will see a message stating that the Remote-Desktop application is not present, to create one with statistics, and to apply the application to all appropriate ICA classifiers.

If the Remote-Desktop application is created but not monitored for statistics, you will see a message stating that the Remote-Desktop application is not collecting statistics, to enable statistics collection in the Remote-Desktop application, and ensure the application is applied to all appropriate ICA classifiers.

ICA Compression Over Time

Figure 3 displays the reduction percentage achieved for the Remote-Desktop application. This chart excludes pass-through traffic in the results.

Figure 3 ICA Compression over Time



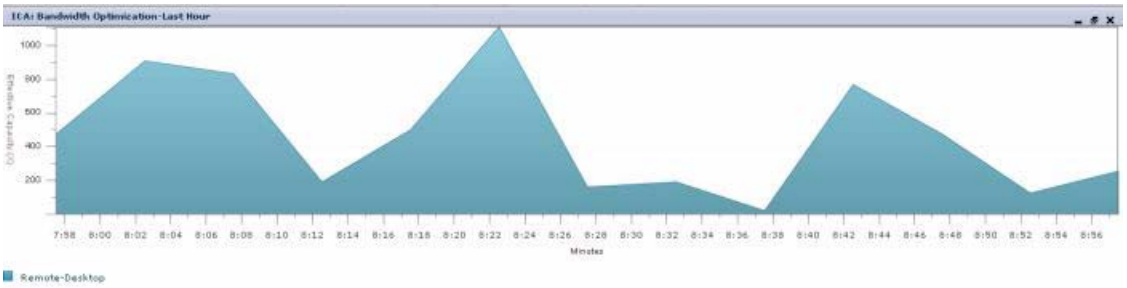
Formula:

% Reduction Excluding Pass-Through = (Original Excluding Pass-Through - Optimized) / (Original Excluding Pass-Through)

ICA Bandwidth Optimization

Figure 4 displays the effective increased bandwidth capacity of the WAN link as a result of Remote-Desktop application traffic optimization. This is an area chart.

Figure 4 ICA Bandwidth Optimization



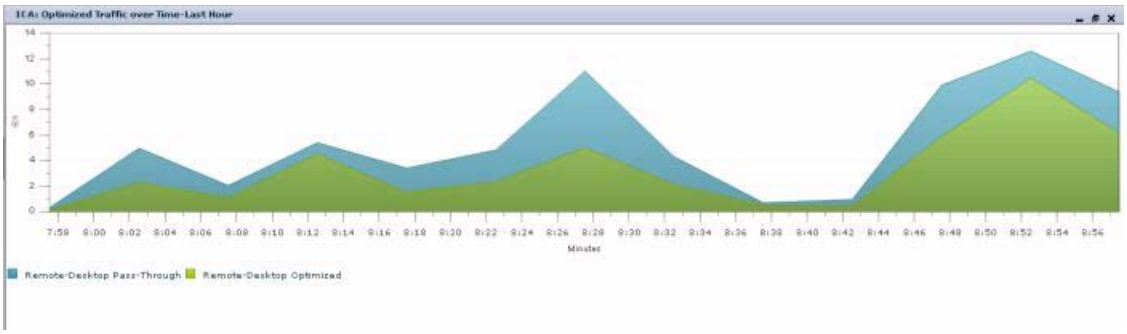
Formulas:

- % Reduction Excluding Pass-Through for Inbound = (Original Outbound - Optimized Inbound - Pass-Through in) x 100 / (Original Outbound - Pass-Through in)
- % Reduction Excluding Pass-Through for Outbound = (Original Inbound - Optimized Outbound - Pass-Through out) x 100 / (Original Inbound - Pass-Through out)
- % Reduction Excluding Pass-Through for System or Bi-directional = (Original Inbound + Original Outbound - Optimized Outbound - Optimized Inbound - Pass-Through out - Pass-Through in) x 100 / (Original Inbound + Original Outbound - Pass-Through out - Pass-Through in)

ICA Optimized Traffic over Time

Figure 5 displays the comparison of the amount of optimized and pass-through traffic of the Remote-Desktop application flowing across the device. The traffic units (bytes, KB, MB, or GB) at the left side depend upon the range. This is an area chart.

Figure 5 ICA Optimized Traffic over Time



ICA Optimized Connections over Time

Figure 6 displays the number of connections optimized for the Remote-Desktop application.

Figure 6 ICA Optimized Connections over Time

Software Version 4.5.1 Filenames

This section describes the WAAS software Version 4.5.1 software image files for use on WAAS appliances and modules and contains the following topics:

- Standard Image Files, page 6
- No Payload Encryption (NPE) Image Files, page 7

Standard Image Files

WAAS software Version 4.5.1 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-4.5.1.*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-4.5.1.*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 an 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-4.5.1.*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-4.5.1.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-4.5.1.*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-4.5.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.5.1.*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 the instructions provided by Cisco TAC.
- waas-alarm-error-books-4.5.1.*x*.zip—Contains the alarm and error message documentation.
- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available at the Cisco Wide Area Application Services (WAAS) Software > Tools directory on Cisco.com.)

No Payload Encryption (NPE) Image Files

WAAS software Version 4.5.1 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-4.5.1.*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-4.5.1.*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-4.5.1.*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-4.5.1.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-4.5.1.*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-4.5.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-4.5.1.*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 the instructions provided by Cisco TAC.
- waas-alarm-error-books-4.5.1.*x*-npe.zip—Contains the NPE alarm and error message documentation.
- virtio-drivers.iso—Virtual blade paravirtualized network drivers for Windows. (Available at 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

For the latest information on WCCP platform support and recommended IOS versions, see: *Cisco Wide Area Application Services Web Cache Communication Protocol Redirection: Cisco Router Platform Support*

Central Managers running Version 4.5.1 can manage WAEs running software Versions 4.0.19 and later. However, we recommend 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 to 0xF00 in Version 4.2.1. 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 Cisco 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 Cisco 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. Because 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 (the 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 4.5.1

To upgrade from WAAS prerelease software to Version 4.5.1, 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 4.5.1

This section contains the following topics:

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

Requirements and Guidelines

When you upgrade to Version 4.5.1, observe the following guidelines and requirements:

- Upgrading to Version 4.5.1 is supported only from Versions 4.1.1d, 4.1.3, 4.1.3b, 4.1.5c, 4.1.5f, 4.1.7, 4.1.7a, 4.1.7b, 4.2.1, 4.2.3, 4.2.3c, 4.3.1, 4.3.3, 4.3.5, 4.4.1, 4.4.3, and 4.4.3a. 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 4.5.1 version.
- Upgrading to Version 4.5.1 is not supported on the following platforms: WAE-511, WAE-611, and WAE-7326. WAAS Version 4.5.1 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.
- Before upgrading a WAAS Central Manager to Version 4.5.1, 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.
- 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.
- 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*.
- When upgrading a WAAS Central Manager to version 4.5.1, the action for Remote-Desktop policies containing citrix-ica, ica, and/or citriximaclient classifiers is updated to: **action optimize full accelerate ica**. In versions earlier than WAAS 4.4, citrix-ica classifier was used for ports 2598 and 1494. In WAAS versions 4.4 and later, ica and citriximaclient classifiers are used.
- If you are upgrading a WAAS Central Manager to version 4.4.1 or later 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 or later, 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 4.5.1, 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 4.5.1, 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 4.5.1, 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 4.5.1, wccp router list 7 is used. Because 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 4.5.1 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 4.5.1 (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 4.5.1 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 4.5.1 device is compatible with all Version 4.1.x, 4.2.x, 4.3.x, and 4.4.x peers, but is not compatible with 4.0.x peers.
- After upgrading WAE devices to Version 4.4.1 or later, 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 4.5.1 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 or later, 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 or later, 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 4.5.1??? 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 or later, 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 later and upgrading to Version 4.4.1 and later 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 and later. On upgrade to Version 4.4.1 and later, 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 or later is done before the data is printed.

  A Version 4.4.1 and later 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 4.1.3 and later support SSL application definition, which is enabled for monitoring by default. However, if you are upgrading from Version 4.1.1 to Version 4.5.1 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 4.5.1, 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 4.5.1, 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 4.5.1, 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 4.5.1, 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.x to Version 4.5.1, 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 to 0xF00 in Version 4.2.1. 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 8.
- 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 4.5.1, 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 4.5.1 to a Previous Version

Note the following guidelines and considerations for downgrading:

- Downgrade is supported only to Versions 4.4.3a, 4.4.3, 4.4.1, 4.3.5, 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.
- All preposition directives configured in CIFS accelerator mode must be removed before downgrading to a version earlier than 4.1.1. You also must configure legacy mode file services by enabling a core server and configuring a WAFS core cluster, enabling an edge server, and registering file servers with the Central Manager.
- All dynamic shares configured in CIFS accelerator mode must be switched to legacy mode before downgrading to a version earlier than 4.1.1, if you want to keep the dynamic shares. To switch a dynamic share to legacy mode, follow these steps:

  1. Edit the dynamic share in the **Configure > File > Dynamic Shares** window and choose a file server in the drop-down list. (File servers must be previously registered in the **Configure > File > File Servers** window.)
  2. Click **Submit**.
- If extended object cache is enabled, all CIFS cache data, DRE cache data, and virtual blade data is lost when downgrading to a version earlier than 4.2.1.
- Any new reports and charts that were introduced in Version 4.5.1 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 4.5.1 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.
- When downgrading a WAAS Central Manager from version 4.5.1, the action for Remote-Desktop policies containing citrix-ica, ica, and/or citriximaclient classifiers is reverted from **action optimize full accelerate ica** to **action optimize full**. In WAAS versions earlier than 4.4, citrix-ica classifier was used for ports 2598 and 1494. In WAAS versions 4.4 and later, ica and citriximaclient classifiers are used.

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 *Cisco Wide Area Application Engine 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 these 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 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 Version 4.5.1 and contains the following topics:

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes Version 4.5.1 devices with devices running earlier software versions.

- WAAS Version 4.5.1 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 4.5.1. 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 4.5.1, 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 4.5.1, 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.

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

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

Internet Explorer Certificate Request

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

Software Version 4.5.1 Resolved Caveats, Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, and command changes in software Version 4.5.1 and contains the following topics:

Software Version 4.5.1 Resolved Caveats

The following caveats were resolved in software Version 4.5.1.

Caveat ID Number	Description
CSCtt32535	Poor Performance & Significant Nack/R-tx Observed After 4.4.x Upgrade

Software Version 4.5.1 Open Caveats

The following open caveats apply to software Version 4.5.1.

Caveat ID Number	Description
CSCtt02028	Client version counter doesn't increment for CGP reconnect
CSCtu26410	Expired CA Verisign needs to be removed from well-known CA list

The additional open caveats for software Version 4.5.1 are the same as those for software Version 4.4.3x, except for those that are resolved in Version 4.5.1. For details, see *The Release Note for Cisco Wide Area Application Services (Software Version 4.4.3x).*

Software Version 4.5.1 Command Changes

This section lists the modified commands in WAAS software Version 4.5.1.

Table 1 lists existing commands that have been modified in WAAS Version 4.5.1.

Table 1 CLI Commands Modified in Version 4.5.1

Mode	Command	Description
EXEC	**clear statistics accelerator ica**	Added **ica** keyword clear ICA accelerator statistics.
	debug accelerator ica [**all** | **ao-connectionmgr** | **ao-parser** | **cgp** | **connection** | **containerring** | **crypto** | **detectionparser** | **failure** | **hash** | **ica** | **initialization** | **io** | **main** | **pipe** | **shell**]	Added **ica** keyword to enable ICA accelerator debugging. The following additional keywords are supported: • **all**—Enables all ICA accelerator debugging. • **ao-connectionmgr**—Enables ICA AO-ConnectionMgr debugging. • **ao-parser**—Enables ICA AO-Parser debugging. • **cgp**—Enables ICA CGP debugging. • **connection**—Enables ICA AO-Connection debugging. • **containerring**—Enables ICA containerring debugging. • **crytpo**—Enables ICA CRYPTO debugging. • **detectionparser**—Enables ICA detectionparser debugging. • **failure**—Enables ICA Allocation failure debugging. • **hash**—Enables ICA HASH debugging. • **ica**—Enables ICA ICA parsing debugging. • **initialization**—Enables ICA initialization debugging. • **io**—Enables ICA IO debugging. • **main**—Enables ICA Main debugging. • **pipe**—Enables ICA PIPE debugging. • **shell**—Enables ICA shell debugging.
	show accelerator	Added ICA accelerator status to output, including license state, config state, and operational state.
	show accelerator ica	Added keyword **ica** to show ICA accelerator status, including license state, config state, operational state, accelerator configuration, and policy engine configuration.
	show statistics connection	Added ICA acceleration type to output: I = ICA.
	show statistics connection conn-id 14259	Added ICA connection information to output.

Table 1 CLI Commands Modified in Version 4.5.1 (continued)

Mode	Command	Description
	show statistics accelerator ica detail	Added **ica detail** keyword to show ICA accelerator statistics detail output: Global Statistics Time Accelerator was started Time Statistics were Last Reset/Cleared Total Handled Connections Total Optimized Connections Total Connections Handed-off with Compression Policies Unchanged Total Dropped Connections Current Active Connections Current Pending Connections Maximum Active Connections Active CGP Connection Active ICA Connections Total CGP Connections Total ICA Connections Total CGP Reconnects Client Version 13.0 Connections Client Version 12.1 Connections Client Version 12.0 Connections Client Version 11.2 Connections Client Version 11.0 Connections Other client version connections Connections No Encryption Connections Basic Encryption Connections RC5 Encryption Connections RC5 Login-Only Encryption Connections Handed-off because of Unrecognized Protocol Connections Handed-off because of Unsupported Client Version Connections Handed-off because of Unknown CGP Session ID Connections Handed-off because of Client on Denied List Connections Handed-off because of Resource Limit Connections Handed-off because of Other Reasons Connections Disconnected because of Unsupported Client Version Connections Disconnected because of I/O Error Connections Disconnected because of Parse Error Connections Disconnected because of Resource Limit Connections Disconnected because of Session In Use Connections Disconnected because of Other Reasons
Global configuration	**accelerator ica enable**	Added **ica enable** keywords to enable the ICA traffic accelerator.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.