



Release Note for Cisco Wide Area Application Services Software Version 4.1.3x

July 31, 2009



Note

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

Contents

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

- 4.1.3b
- 4.1.3a
- 4.1.3

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 from a Prerelease Version to Version 4.1.3x](#)
- [Upgrading from Version 4.0.x or 4.1.1x to 4.1.3x](#)
- [Downgrading from Version 4.1.3b to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade](#)



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

- [Cisco WAE-612 Hard Disk Drive Replacement Notification](#)
- [Operating Considerations](#)
- [Software Version 4.1.3b Resolved and Open Caveats](#)
- [Software Version 4.1.3a Resolved and Open Caveats](#)
- [Software Version 4.1.3 Resolved Caveats, Open Caveats, and Command Changes](#)
- [WAAS Documentation Set](#)
- [Obtaining Documentation and Submitting a Service Request](#)

New and Changed Features

The following sections describe the new and changed features and functionality in software version 4.1.3x:

- [Software Version 4.1.3b Functionality Changes](#)
- [Software Version 4.1.3a Functionality Changes](#)
- [Software Version 4.1.3 New and Changed Features](#)

Software Version 4.1.3b Functionality Changes

- CIFS preposition operation has been altered to allow concurrent preposition tasks.

Software Version 4.1.3a Functionality Changes

- WAAS software version 4.1.3a includes a functionality change for Central Manager usernames. Usernames are now case sensitive.
- CIFS preposition operation has been altered to streamline concurrent preposition tasks from one or more branches in a serialized manner at the core WAAS device. Depending on the actual preposition usage and number of concurrent tasks scheduled, you may notice an increase in time for all concurrent tasks to execute or complete.

Software Version 4.1.3 New and Changed Features

WAAS software version 4.1.3 includes the following new features and changes:

- **SSL application accelerator**—The new SSL application accelerator optimizes traffic on Secure Sockets Layer (SSL) encrypted connections. The SSL application accelerator provides a scalable, secure vault for server private keys and certificate management so that the WAAS software can optimize the traffic on the SSL link while maintaining the security of the connection. A new application definition named SSL was created and the HTTPS classifier was associated with this application. The WAAS Central Manager includes several new SSL configuration pages and there are corresponding new CLI commands.
- **Application accelerators**—All application accelerators were improved to increase stability and performance.

- Video accelerator—The video accelerator handling of unaccelerated traffic was enhanced to allow dropping traffic that is unaccelerated only due to an overload condition.
- Traffic Optimization—Basic traffic optimization including TFO, DRE, and LZ was improved to increase stability and performance.
- Monitoring and reporting—WAAS Central Manager monitoring and reporting capabilities were improved with new and reorganized charts and graphs, and better statistical reporting. Additionally, several CLI show commands were improved with additional output fields.
- WAAS Central Manager usability—The WAAS Central Manager was improved in many areas to increase usability and scalability. Certain functions were renamed and reorganized into different groups or drawers in the navigation pane.
- Virtualization—Virtual blade capabilities were expanded to allow additional virtual blades and lower the memory requirements, depending on the hardware platform. A new WAAS Central Manager window allows you to copy disk images to a virtual blade and back up and restore virtual blades. A Refresh button was added in the virtual blade Actions window to refresh the virtual blade status. To improve security, a new CLI command allows you to disable the VNC server on a virtual blade.
- WCCP configuration—The WAAS Central Manager WCCP configuration pages were consolidated and improved to simplify the WCCP configuration.
- Secure store—The secure store initialization procedure was improved so that initializing the secure store also opens it, making it unnecessary to perform a second step to open it. In addition, a WAAS Central Manager page was added to allow you to initialize and open the secure store and change the password. A new CLI command allows you to reset the secure store in case you forget the password.
- System properties—New system properties were added to set the maximum number of concurrent WAAS Central Manager sessions permitted for a user, to configure a filter for Central Manager input fields, and to configure the replication of statistics data to a standby Central Manager.
- Interface configuration—The new src-dst-ip-port option replaces dst-ip as a method of port channel load balancing. Additionally, you can configure only a single standby interface group, rather than four groups.
- Disk error handling—Disk error handling is now automatic and so the threshold and reload settings are no longer configurable.
- CLI commands—For CLI command changes, see the [“Software Version 4.1.3 Command Changes” section on page 18](#).
- Monitoring API—For Monitoring API changes, see the [“Software Version 4.1.3 Monitoring API Changes” section on page 20](#).

Upgrading From WAFS to WAAS

Although WAFS to WAAS migration is supported, a rollback from WAAS to WAFS is not supported. For information regarding a WAFS-to-WAAS migration, contact your Cisco Sales Engineer.

If you are upgrading from WAFS 3.0.7 or later to WAAS, you must upgrade to a released WAAS version; you cannot upgrade to a prerelease version of WAAS software.

If you are upgrading from the WAFS 3.0.7-special5 build or from a later WAFS release to WAAS, you must upgrade to a minimum of WAAS 4.0.5 or later; however, to ensure that you obtain all of the latest fixes and features, we recommend that you upgrade to the most current version of WAAS.

Note the following points when upgrading from WAFS to WAAS:

- When you upgrade from WAFS to WAAS, you may lose up to half of the WAFS cache space because the upgrade process uses the WAFS cache eviction process to reclaim the space needed for the DRE cache; the oldest content is removed first.
- The hardware that supports WAFS 3.0 also supports WAAS, with the exception of the NM-CE.
- You need a dedicated WAE to function as the Central Manager in WAAS.
- You must place the WAEs in a separate subnet from the clients, or you must use the GRE return feature.
- After migrating from WAFS to WAAS, reenter the file server credentials from the WAAS Central Manager GUI.

Upgrading from a Prerelease Version to Version 4.1.3x

To upgrade from WAAS prerelease software to version 4.1.3x, you must perform the following tasks to ensure a successful upgrade:

- Restore the factory default settings by using the **restore factory-default** command.
- Perform a fresh install from the rescue CD.

Upgrading from Version 4.0.x or 4.1.1x to 4.1.3x

This section contains the following topics:

- [Requirements and Guidelines](#)
- [Ensuring a Successful RAID Pair Rebuild](#)
- [Managing Passwords after an Upgrade](#)

Requirements and Guidelines

When you upgrade from version 4.0.x or 4.1.1x to version 4.1.3x, observe the following guidelines and requirements:

- 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.
- Upgrading to version 4.1.3x is supported only from version 4.0.13 and later. If you want to upgrade WAAS devices running earlier versions, first upgrade them to version 4.0.13, 4.0.17 or 4.0.19, then to 4.1.3x.
- Upgrade the WAAS Central Manager devices first, and then upgrade the WAE devices. If you have a standby WAAS Central Manager, upgrade it first, before upgrading the primary WAAS Central Manager. After upgrading, restart any active browser connections to the WAAS Central Manager.

- Before upgrading a WAAS Central Manager to version 4.1.3x, make a database backup by using the **cms database backup** EXEC command. This command creates a backup file in /local1/. In case of any problem during the upgrade, you can restore the database backup that you made before upgrading by using the **cms database restore** *backup-file* EXEC command, where *backup-file* is the one created by the backup command.
 - If you upgrade a WAAS Central Manager to 4.1.3b using the **Jobs > Software Update** page from a 4.0.x WAAS Central Manager, enter 4.1.3.b.6 in the Software Version field.
 - After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If WAFS was enabled on the device before the upgrade, then the Enterprise license should be enabled. Configure any additional licenses (Video and Virtual-Blade) as needed by using the **license add** EXEC command. For more information on licenses, see the “[Managing Software Licenses](#)” section on page 9-3 in the *Cisco Wide Area Application Services Configuration Guide*.
 - After upgrading application accelerator WAEs, verify that the proper application accelerators, policies, and classifiers are configured. For more information on configuring accelerators, policies, and classifiers, see [Chapter 12, “Configuring Application Acceleration”](#) in the *Cisco Wide Area Application Services Configuration Guide*.
 - WAAS version 4.1.3 introduces the new SSL application definition, which is enabled for monitoring by default. However, if you are upgrading to version 4.1.3 from an earlier version and already have 20 applications enabled for monitoring, the new SSL application will have monitoring disabled because a maximum of 20 monitored applications are allowed. In order to enable monitoring of the SSL application, you must disable monitoring of a different application and then enable monitoring of the SSL application. You can enable and disable monitoring by using the Enable Statistics check box in the Modifying Application page of the WAAS Central Manager (**Configure > Acceleration > Applications > Application Name**).
- If the SSL Bandwidth Optimization chart has no data, then monitoring may be disabled for the SSL application definition. Check that monitoring is enabled for the SSL application.
- WAAS version 4.1.3x supports strong passwords. When you upgrade from version 4.0.17 or an earlier version, which does not support strong passwords, the previous weaker passwords will be retained. For details, see the “[Managing Passwords after an Upgrade](#)” section on page 7.
 - If you are upgrading a WAAS Central Manager from version 4.0.19 or later and have the secure store enabled, you will need to reopen the secure store after the device reloads (and after any reload). From the WAAS Central Manager GUI, choose **Admin > Secure Store** or use the **cms secure-store open** EXEC command. For more information on using the secure store, see the “[Configuring Secure Store Settings](#)” section on page 9-10 in the *Cisco Wide Area Application Services Configuration Guide*.
 - If you are upgrading a WAE-511 or WAE-611, ensure that the BIOS disk mode is set to Native.
 - When upgrading a WAE from version 4.0.19 or earlier to version 4.1.3x, where the default policy configuration was applied from the CLI, after the upgrade, you may see two classifiers for NFS traffic in the WAAS Central Manager and on the WAE device: NFS and NFS-non-wafs. This has no effect on NFS traffic acceleration, which continues to operate as configured.
 - If you are upgrading from version 4.0.x to version 4.1.x, the way a wildcard mask is interpreted has changed. Wildcard masks can be specified for a traffic classifier match condition or an ACL rule. In version 4.0.x, a wildcard mask of 255.255.255.255 would (incorrectly) match no IP addresses, but in version 4.1.x, this wildcard mask matches any IP address, as expected.

- The device group and role naming conventions have changed in version 4.1.3. Device group and role names cannot contain characters other than letters, numbers, period, hyphen, underscore, and space. (In version 4.0.x, other characters were allowed.) If you upgrade from version 4.0.x to version 4.1.3x, disallowed characters in device group and role names are retained, but if you try to modify the name, you must follow the new naming conventions.
- The standby interface configuration changed in version 4.1.3. If multiple standby groups are configured before upgrading, only the group with the lowest priority and a valid member interface will remain after the upgrade, and it will become standby interface 1. If the errors option was configured, it will be removed.
- If you have two Central Managers that have secure store enabled and you have switched primary and standby roles between the two Central Managers, before upgrading the Central Managers to version 4.1.3, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords, CIFS file server passwords, and WAFS core passwords. If you do not reenter the passwords, after upgrading to version 4.1.3, the Central Manager will fail to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you have a version 4.1.1x Central Manager where secure store has been initialized but not opened (such as after a reload) and the Central Manager has sent configuration updates containing user account, CIFS core password, preposition, or dynamic share changes to WAEs before the secure store was opened, then before upgrading the Central Manager to version 4.1.3, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords, CIFS file server passwords, and WAFS core passwords. If you do not reenter the passwords, after upgrading to version 4.1.3, the Central Manager will fail to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you have a version 4.1.1x or earlier Central Manager, are using external/remote users that have the admin role, and have edited one or more of these users on the Central Manager, you might encounter caveat CSCsz24694, which causes the Central Manager not to send updates to WAEs after upgrading to version 4.1.3. 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. This issue is resolved in version 4.1.3a and later.
- If you are upgrading a standby Central Manager from version 4.1.1c or 4.1.1d to 4.1.3x, and it has been running for more than three months, the upgrade could fail due to a large database size. In this situation, we recommend that you follow these steps:
 1. Deregister the standby Central Manager.
 2. Upgrade the standby Central Manager.
 3. Upgrade the primary Central Manager.
 4. Register the standby Central Manager with the primary Central Manager.

Ensuring a Successful RAID Pair Rebuild

RAID pairs will rebuild on the next reboot after you use the **restore factory-default** command, replace or add a hard disk drive, delete disk partitions, or reinstall WAAS from the booted recovery CD-ROM.



Caution

You must ensure that all RAID pairs are done rebuilding before you reboot your WAE device. If you reboot while the device is rebuilding, you risk corrupting the file system.

To view the status of the drives and check if the RAID pairs are in “NORMAL OPERATION” or in “REBUILDING” status, use the **show disk details** command in EXEC mode. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process may take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms that could indicate a problem:

- The device is offline in the Central Manager GUI.
- CMS cannot be loaded.
- Error messages say that the file system is read-only.
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” or “ext3_readdir: bad entry in directory.”
- Other unusual behaviors occur that are related to disk operations or the inability to perform them.

If you encounter any of these symptoms, reboot the WAE device and wait until the RAID rebuild finishes normally.

Managing Passwords after an Upgrade

WAAS software version 4.1.3x includes a strong password feature for improved security. Versions of the WAAS software previous to 4.0.19 do not have a strong password capability.



Note

The following considerations apply to WAAS software version 4.1.3x with the strong password policy enabled. Strong passwords are disabled by default.

When you upgrade from version 4.0.17 or earlier to version 4.1.3x, note the following password considerations:

- Existing passwords from the older version will continue to work in version 4.1.3x.
- Existing passwords will expire after 90 days. Subsequent new passwords must conform to strong password requirements.
- Strong passwords must meet the following requirements:
 - The password must be 8 to 31 characters long.
 - The password can include both uppercase and lowercase letters (A–Z and a–z), numbers (0–9), and special characters including ~!@#%&*()_+=[\] ; : < / > .
 - The password cannot contain the characters ` ` | (apostrophe, double quote, or pipe) or any control characters.
 - The password cannot contain all the same characters (for example, 99999).
 - The password cannot contain consecutive characters (for example, 12345).
 - The password cannot be the same as the username.

Downgrading from Version 4.1.3b to a Previous Version

Note the following guidelines for downgrading:

- Downgrade is supported only to versions 4.1.3a, 4.1.3, 4.1.1d, 4.1.1c, 4.1.1b, 4.1.1a, 4.1.1, 4.0.25, 4.0.23, 4.0.21, 4.0.19, 4.0.17, or 4.0.13.

- 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 enable features such as secure storage and strong passwords in version 4.1.3x, you must disable them before you downgrade WAAS to a previous version (4.0.13 or 4.0.17) that does not support them.
- Locked-out user accounts will be reset upon downgrade.
- All preposition directives configured in CIFS accelerator mode must be removed before downgrading to a version prior to 4.1.1. You also must configure legacy mode file services by enabling a core server and configuring a WAFS core cluster, enabling an edge server, and registering file servers with the Central Manager.
- All dynamic shares configured in CIFS accelerator mode must be switched to legacy mode before downgrading to a version prior to 4.1.1, if you want to keep the dynamic shares. To switch a dynamic share to legacy mode, follow these steps:
 1. Edit the dynamic share in the **Configure > File > Dynamic Shares** window and choose a file server in the drop-down list. (File servers must be previously registered in the **Configure > File > File Servers** window.)
 2. Click **Submit**.

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.1.3a, 4.1.3, 4.1.1d, 4.1.1c, 4.1.1b, 4.1.1a, 4.1.1, 4.0.25, 4.0.23, 4.0.21, 4.0.19, 4.0.17, or 4.0.13, follow these steps:

-
- Step 1** (Optional) If secure store is enabled, disable it using the **cms secure-store clear** global configuration command.
- ```
(config)# cms secure-store clear
```
- Step 2** From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device.
- ```
CentralManager# cms database backup
```
- Step 3** (Optional) If you are downgrading from a fresh install of version 4.1.3x (from the factory or from an installation performed with the WAAS recovery CD), back up the downgrade scripts to an FTP server as follows:
- a. Enable FTP on the WAAS Central Manager by using the **inetd enable ftp** global configuration command.
 - b. Copy the needed downgrade scripts to the FTP server by using the **copy disk** EXEC command, as shown in the following example:


```
CentralManager# copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_3_to_4_1_1c
downgrade/WAAS_Downgrade4_1_3_to_4_1_1c
```

You need to copy only the downgrade scripts that you intend to use. See [Step 7](#) for the complete list of downgrade scripts available.
- Step 4** Install the downgrade WAAS software image by using the **copy ftp install** EXEC command.
- Step 5** Reload the device.
- The database needs to be downgraded before the Central Manager can use it and the CMS process can start. To optionally verify this status, use the **show cms info** EXEC command. It should respond with a message saying that a database downgrade is required.

Step 6 (Optional) If you performed [Step 3](#), then restore the downgrade script files from the FTP server where you backed them up to the /downgrade directory on the WAAS Central Manager by using the **copy ftp EXEC** command as follows:

```
CentralManager# copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_3_to_4_1_1c
downgrade/WAAS_Downgrade4_1_3_to_4_1_1c
```

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

```
CentralManager# cms database downgrade script downgrade/WAAS_Downgrade4_1_3_to_4_1_1c
```

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



Note If you are downgrading from version 4.1.3b to version 4.1.3a or 4.1.3, no script is necessary. However, you must still execute the **cms database downgrade** command.

- WAAS_Downgrade4_1_3_to_4_0_13
- WAAS_Downgrade4_1_3_to_4_0_17
- WAAS_Downgrade4_1_3_to_4_0_19
- WAAS_Downgrade4_1_3_to_4_0_21
- WAAS_Downgrade4_1_3_to_4_0_23 (also use this script when downgrading to 4.0.25)
- WAAS_Downgrade4_1_3_to_4_1_1
- WAAS_Downgrade4_1_3_to_4_1_1a
- WAAS_Downgrade4_1_3_to_4_1_1b
- WAAS_Downgrade4_1_3_to_4_1_1c
- WAAS_Downgrade4_1_3_to_4_1_1d

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

```
config
(config)# cms enable
```

Downgrading the database may trigger full updates for registered devices. In the Central Manager GUI, ensure that all previously operational devices come online.

Cisco WAE and WAVE Appliance Boot Process

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

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

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

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

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

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

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

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on cisco.com at the [Cisco Wide Area Application Engine \(WAE\) Utilities Software Downloads \(registered customers only\)](#) page. The firmware binary image is named L4_15427_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware and are named L4_15427_FIRMWARE.pdf.

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 4.1.3x:

- [Interoperability](#)
- [Device Group Default Settings](#)
- [Using Autoregistration with Port-Channel Interfaces](#)
- [WAFS Support of FAT32 File Servers](#)

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.1.3x devices with devices running earlier software versions.

- WAAS version 4.1.3x does not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.13. If you have any WAAS devices running version 4.0.11 or earlier, you must first upgrade them to version 4.0.13 (or a later version), before you install version 4.1.3x. You should first upgrade any WAEs to version 4.0.13 (or a later version) and then upgrade any WAAS Central Managers to version 4.0.13 (or a later version).
- In a mixed version WAAS network with version 4.1.3x, the WAAS Central Manager must be running the highest version of the WAAS software.
- When a WAAS Central Manager is upgraded to version 4.1.3x and it is managing a 4.0.x device with legacy mode WAFS enabled that is not upgraded, the device may appear to have both legacy mode WAFS and the transparent CIFS accelerator enabled, because the Central Manager enables it by default. Disable the transparent CIFS accelerator if you want to continue to use legacy mode for WAFS.

Device Group Default Settings

When you create a new device group in WAAS version 4.1.3x, the **Configure > Acceleration > DSCP Marking** page is automatically configured for the group, with the default DSCP marking value of copy.

Using Autoregistration with Port-Channel Interfaces

Do not enable the **auto-register** global configuration command when both interfaces are configured as port-channel interfaces.

WAFS Support of FAT32 File Servers

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

Software Version 4.1.3b Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.3b:

- [Software Version 4.1.3b Resolved Caveats, page 11](#)
- [Software Version 4.1.3b Open Caveats, page 12](#)

Software Version 4.1.3b Resolved Caveats

The following caveats were resolved in software version 4.1.3b.

Caveat ID Number	Description
CSCsz13456	WAVE-574 log is flooded with IPMI BMC messages
CSCsz53126	Preposition with large number of files in a root share may not complete
CSCsz84284	Preposition task may not complete for root shares with many files

Caveat ID Number	Description
CSCsz86878	CM may fail to upgrade rarely when there are huge unused db records.
CSCta42359	WAAS: license failure alarm may be generated for a valid license
CSCtb01489	WAE loses network connectivity after changing network interface settings

Software Version 4.1.3b Open Caveats

The following open caveats apply to software version 4.1.3b.

Caveat ID Number	Description
CSCsz48025	CM GUI Preposition status page, scroll bar and pagination is not working
CSCta21795	Rarely WAE could kdump and reboot during internal connection setup
CSCta25256	When radius server down, failover to local authentication fails.
CSCta27573	Under certain conditions, config update between CM and WAE may fail
CSCta28526	CM GUI progress bar not in sync with page load status on IE6 SP3 browser
CSCta36082	Enhance connection statistics to show all info pertaining to box limit
CSCta38419	Under rare conditions VB may crash when a RAID disk fails
CSCta44714	Core file generated during image downgrade upon disk failure
CSCta55041	Preposition task may terminate with reason as "Internal Error"
CSCta58662	CM is unresponsive when modifying dynamic share under huge configuration
CSCta58682	4.1.1x Standby CM upgrade may fail under certain conditions
CSCta77941	WAE loses static routes when Standby interface members removed and added
CSCta94350	Under rare conditions, CM key manager may fail to serve keys to WAEs.
CSCtb10372	Rarely, WAE may lose connectivity temporarily after registration to CM

The additional open caveats for software version 4.1.3b are the same as those for software version 4.1.3a, with the exception of CSCsz86878 and CSCsz84284, which are resolved for 4.1.3b. For details, see the [“Software Version 4.1.3a Open Caveats”](#) section on page 13.

Software Version 4.1.3a Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.3a:

- [Software Version 4.1.3a Resolved Caveats, page 13](#)
- [Software Version 4.1.3a Open Caveats, page 13](#)

Software Version 4.1.3a Resolved Caveats

The following caveats were resolved in software version 4.1.3a.

Caveat ID Number	Description
CSCsw36112	File preposition may not complete when very large files are transferred
CSCsx54846	Preposition task may not complete under specific stress scenario
CSCsy19889	WCCP bucket assignments issue during multiple changes in farm.
CSCsz00205	Quickbooks application becomes unresponsive when optimized through WAE
CSCsz01264	Preposition tasks fail while multiple WAEs scan same high-volume root
CSCsz13297	NME 502 system creates a kdump file and reboots in specific condition
CSCsz24694	CM won't update WAEs after upgrade when users added in a particular way
CSCsz44589	User authorization from CM GUI is case insensitive.
CSCsz51698	In rare client conn patterns & overload, emails duplicate or send fails
CSCsz73200	Auto registration not getting IP from DHCP after reload
CSCsz75377	WAAS - WAE creates vmcore file and restarts in a specific scenario
CSCsz78799	Concurrent preposition tasks may not fetch all the data for large files
CSCta04789	File server keepalives may stop with concurrent preposition

Software Version 4.1.3a Open Caveats

The following open caveats apply to software version 4.1.3a.

Caveat ID Number	Description
CSCsz21500	NetBIOS name was returned to one at boot up after NetBIOS name change
CSCsz22079	In very rare cases, Outlook clients may need to reconnect
CSCsz25404	Some CIFS AO expert-mode configuration is not persistent
CSCsz31059	CIFS Ao sevice disabled alarm seen on NME-502 after upgarde from 4.0.23
CSCsz31354	Under rare scenario user may need to retry file access with SMB signing
CSCsz72205	Switching device in CIFS acceleration report results in error message
CSCsz72423	WAAS print services not refreshing printers DNS entries
CSCsz77090	SSL connections can fail to close after long periods of oversubscription
CSCsz79689	WAE creates kdump file and reboots in special condition
CSCsz79863	Preposition task failed to fetch all the files after network disruption
CSCsz84284	Preposition task may not complete for root shares with many files
CSCsz86527	Preposition tasks may fail to fetch data in rare condition
CSCsz86878	CM may fail to upgrade rarely when there are huge unused db records
CSCsz87027	In rare cases, SNMP client may need to retry requests
CSCsz93357	Preposition tasks may abort with "internal error" on reschedule

Caveat ID Number	Description
CSCsz93401	Preposition tasks may fail to complete on reschedule
CSCta06716	Under rare conditions, Java core dump occurs on WAE post reload
CSCta06901	Samba clients talking to Samba server may see directory browsing errors
CSCta18195	WAAS resets HTTP CONNECT with mixed 4.1.1 and 4.1.3 versions
CSCta28526	Preposition page may not load completely while using specific browsers

The additional open caveats for software version 4.1.3a are the same as those for software version 4.1.3, with the exception of CSCsw36112 and CSCsz24694, which are resolved for 4.1.3a. For details, see the [“Software Version 4.1.3 Open Caveats”](#) section on page 16.

Software Version 4.1.3 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.1.3:

- [Software Version 4.1.3 Resolved Caveats, page 14](#)
- [Software Version 4.1.3 Open Caveats, page 16](#)
- [Software Version 4.1.3 Command Changes, page 18](#)

Software Version 4.1.3 Resolved Caveats

The following caveats were resolved in software version 4.1.3.

Caveat ID Number	Description
CSCso16224	winbindd core file is generated when data center WAE is restarted
CSCsr76755	"Roles changed, reload required" alarm seen upon upgrade of edge / core
CSCsr81203	Clients with 64bit XP/VISTA OS cannot print with Print AO
CSCsr91207	Policy definition page is not refreshed after swapping device group.
CSCsr95819	CIFS AO: Not all the expected files are cached by preposition task.
CSCsu02341	Scheduled report fails if the device name contains any device group name
CSCsu31016	DSCP is incorrectly marked as configured in default device group
CSCsu65362	CM core file may be generated on receiving an invalid cookie
CSCsu79552	Amount copied field in GUI may display zero for prepositioning
CSCsu80800	system processes may restart when WAE runs out of memory
CSCsu81277	Connection optimization failure due to peer version mismatch error
CSCsu83896	Rarely when auto activation is enabled CM is unable to configure WAEs.
CSCsu92726	'show statistics' CLI may become unresponsive under heavy load
CSCsu99458	Show tech displays interfaces as shutdown when up and running

Caveat ID Number	Description
CSCsv01550	CPU statistics are inconsistent between CM GUI, Device GUI and SNMP
CSCsv07544	Inline WAE creates kdump file and reboots under high traffic load
CSCsv12397	Optimization charts are not plotted correctly in custom time zone
CSCsv31637	Java core file is created under heavy CIFS traffic
CSCsv37977	Directory traversal sequence may allow user to read arbitrary files
CSCsv38726	CM GUI generates Null pointer exception while accessing CIFS AO charts
CSCsv43859	Under certain conditions, Java core generated on WAE
CSCsv44335	CIFS AO becomes unresponsive due to out of memory
CSCsv48256	Request manager error causes CIFS AO to restart under heavy load
CSCsv51243	CM exception is generated while viewing scheduled reports table
CSCsv54486	System message seen while exporting the CSV for any CIFS charts
CSCsv54569	Under certain conditions, not able to enable SSH from CM GUI
CSCsv54772	Cannot configure policy map by setting both passthrough and accelerate
CSCsv57007	With HTTP AO core WAE creates core file and reboots
CSCsv64485	nscd service disabled under heavy load
CSCsv73453	Exceptions are seen when Non Admin user views a report created by admin
CSCsv77888	Under certain conditions, not able to view TCP statistics print report.
CSCsv80627	Inconsistent view of WCCP farm leads to traffic bypassing WAE's
CSCsv82775	Mode switch from legacy CIFS to CIFS AO not working properly
CSCsv84280	In CM GUI, custom time settings of CPU statistics graph does not work
CSCsv85781	CM GUI has slow response in certain conditions
CSCsv85910	CM GUI issues with IE - printing of group policy defs not working
CSCsv89088	In particular scenario, not able to enable CMS service on WAE.
CSCsv89200	Local user with print role is not able to view / edit print pages
CSCsv90303	Stale print jobs may be found in print spool directory with legacy print
CSCsv94002	Java core file is generated while monitoring connection stats from CM
CSCsv97802	Unable to login to CM GUI with password length more than 20 characters.
CSCsw18374	MAPI AO restarts unexpectedly in rare conditions
CSCsw23864	System creates a core file and reloads when connections are reset
CSCsw29179	Negative values shown in DRE detailed statistics under heavy load
CSCsw30182	System creates a kdump file and reboots under heavy MAPI load
CSCsw33145	Legacy CIFS Edge service becomes unresponsive and restarts under heavy traffic
CSCsw37661	Unable to browse directory with CIFS prepositioned content
CSCsw39707	Configured Virtual Blade interface not restored after reloading WAE
CSCsw39896	CIFS Preposition directive gets renamed when configured from CLI
CSCsw47337	WAAS-Throughput for CIFS connections can be low under certain conditions
CSCsw51721	CIFS AO does not start on NM when the AO has timed out

Caveat ID Number	Description
CSCsw63080	WAE generates an alarm on CM that core files are created
CSCsw80798	CIFS preposition tasks fail with NTLMv2 authentication
CSCsw81143	Device GUI sysreport generation may timeout
CSCsw81310	CM GUI - Pagination is not working in print servers page
CSCsw85346	MAPI AO may create a core file when packet arrives on expired session
CSCsw96856	With CIFS exception is written and may reload under heavy load
CSCsx00906	Previously assigned print role to user may not take effect after upgrade
CSCsx15577	CM service restarts when the its log file reaches 2GBsize
CSCsx16177	Cannot add preposition same as existing preposition from another WAE CLI
CSCsx17824	Multiple instances of same chart in a report results in improper values
CSCsx34060	Static routes defined in config not working after reload
CSCsx36792	Under certain conditions, unable to select Feb month from calendar icon
CSCsx42080	WAE generates SNMP core file and reloads in rare circumstances
CSCsx47449	WAE fails to reload automatically after the scheduled time period
CSCsx60782	Traffic disruption seen on WAE-7371 after RAID controller failed
CSCsx68058	Routing loops at the core can cause TFO overload on the WAE
CSCsx76824	Management service is unable to start after CM backup is restored
CSCsx82342	FTP clients may not receive the complete file in rare conditions
CSCsy08601	Modification of VB config from CM will erase multiple disk configuration
CSCsy18859	WAE may generate MAPI core file in rare circumstances
CSCsy20228	Under rare conditions, viewing UI pages leads to CMS service restart.
CSCsy22506	With CIFS AO Windows Resource Kit commands may not succeed
CSCsy42027	Exceptions may be generated while configuring TFO policies
CSCsy82086	WAAS default gateway removed from routing table after reload of NME-WAE

Software Version 4.1.3 Open Caveats

The following open caveats apply to software version 4.1.3.

Caveat ID Number	Description
CSCsu08094	Force Device Group icon appears in device group config on upgrade
CSCsu62467	Java core file is generated when WAE reboots
CSCsv23571	CIFS AO restarts due to liveness alarms under heavy load
CSCsv40789	Tethereal read filter is not applied if capture data is written to file
CSCsw36112	File preposition may not complete when very large files are transferred
CSCsw94689	OS/2 clients cannot access file server when using CIFS AO
CSCsx20121	Role change of logged in admin user may result in HTTP errors

Caveat ID Number	Description
CSCsx20509	Preposition status is seen as in progress even when it is disabled in CM
CSCsx22929	Outlook2K clients can't move group of mails between folders with MAPI AO
CSCsx26035	Stopping CIFS AO raises "tfo_accl_wellness" + "wafs_roles_change" alarm
CSCsx31227	Secondary IP address can't be modified for Inline interface from CM GUI
CSCsx41113	Read only users are allowed to edit Save and Save As tabs in Reports
CSCsx54754	Large CIFS preposition configuration not fully applied on device reload
CSCsx58323	Under rare conditions after system startup Device GUI is not accessible
CSCsx58793	CM may display error when diagnostic tool is run with specific versions
CSCsx58948	Connections initiated by Backup Applications may not succeed
CSCsx60778	CMS secure store cannot be opened on WAE when configured from CM GUI
CSCsx60929	Configuring CIFS dynamic share name with space may not succeed in CM
CSCsx64593	CIFS AO may be restarted when CIFS cache is evicting data
CSCsx64796	CIFS AO may generate core on large print jobs while low on memory
CSCsx69046	Non SSL traffic on port 443 is incorrectly counted as reset connections
CSCsx74221	Directed Mode with GRE return may cause high CPU utilization on routers
CSCsx74753	Preposition name is treated as case sensitive in CM GUI
CSCsx77025	Preposition configurations overridden by CM, when CM comes back online
CSCsx78566	Under rare conditions, cannot delete dynamic shares from the CM
CSCsx81460	Exception might be seen while switching between CIFS AO and legacy CIFS
CSCsx96126	Exception seen when no share or "/" is specified as root for Preposition
CSCsx99197	Add chart icon is missing in the device CPU statistics page.
CSCsy03347	Read only user cannot view certain WCCP settings
CSCsy06228	Device policy definition page goes to override mode in specific scenario
CSCsy06780	Use of quotes in certain fields in CM causes navigation/page load issues
CSCsy19655	Scheduled reports might show exceptions when CM changes role
CSCsy19941	Scheduled reports are not generated after upgrade
CSCsy27025	Multiple root shares in a CIFS preposition tasks may lead to failures
CSCsy30310	"show crypto" commands for level 0 user gives error message
CSCsy39729	Winbind core file is created on WAE when domain controller is restarted
CSCsy44915	Power Supply alarm wrongly raised instead of raid_rebuild_abort alarm
CSCsy50180	Device group policy definition is overridden under certain conditions
CSCsy58389	TACACS attribute configuration with symbol '*' is ignored by CM GUI
CSCsy92444	In rare conditions with MAPI AO Outlook 2003 client might display errors
CSCsy93159	EPM AO may generate core file due to certain RPC traffic
CSCsy93922	Windows remote console does not go through when CIFS AO is enabled
CSCsz24694	CM won't update WAEs after upgrade when users added in a particular way

Software Version 4.1.3 Command Changes

This section lists the new, modified, and removed commands in WAAS software version 4.1.3.

[Table 1](#) lists the new commands and options that have been added in WAAS software version 4.1.3.

Table 1 *CLI Commands Added in Version 4.1.3*

Mode	Command and Syntax
EXEC	crypto delete
	crypto export
	crypto generate
	crypto import
	crypto pki
	show statistics connection auto-discovery
Global configuration	accelerator ssl
	crypto pki
	crypto ssl
PKI certificate authority configuration ¹	ca-certificate
	description
	revocation-check
PKI global settings configuration ²	ocsp
	revocation-check
Virtual blade configuration ³	vnc

1. PKI certificate authority configuration commands are used to configure public key infrastructure (PKI) encryption certificate authorities.
2. PKI global settings configuration commands are used to configure OCSP and revocation checking.
3. Virtual blade configuration commands are used to configure virtual blades on platforms that support virtual blades.

Table 2 lists existing commands that have been modified in WAAS version 4.1.3.

Table 2 CLI Commands Modified in Version 4.1.3

Mode	Command and Syntax	Description
EXEC	clear statistics	Added the all and blacklist options to the auto-discovery option.
	clear statistics accelerator	Added the ssl option.
	clear statistics connection	Added the ssl option.
	cms database backup	Added the WAAS version number to the database filename.
	cms secure-store	Added the reset option. Also, the init option now opens the secure store.
	cpfile	Changed from user to privileged EXEC mode.
	delfile	Changed from user to privileged EXEC mode.
	deltree	Changed from user to privileged EXEC mode.
	mkdir	Changed from user to privileged EXEC mode.
	mkfile	Changed from user to privileged EXEC mode.
	rename	Changed from user to privileged EXEC mode.
	rmdir	Changed from user to privileged EXEC mode.
	show cdp	Added InlinePort options to the interface and neighbors options.
	show disks	Added new error information to output.
	show interface	Removed the ability to specify more than one port channel or standby group. Added new output field.
	show statistics accelerator http	Added new output fields.
	show statistics accelerator mapi	Added units to output fields.
	show statistics accelerator nfs	Added new output fields.
	show statistics accelerator ssl	Added the ssl option.
	show statistics accelerator video	Minor output changes.
	show statistics auto-discovery	Added new output fields.
	show statistics cifs	Changed the name of the cache eviction option to cache details .
	show statistics connection	Added new output fields.
	show statistics connection auto-discovery	Added new output fields.
	show statistics connection closed	Added the ssl option and new output fields.
	show statistics connection optimized	Added the ssl option and new output fields.
show statistics connection pass-through	Added new output fields.	
show statistics generic-gre	Added new output field.	
show statistics tfo	Added and changed output fields.	

Table 2 *CLI Commands Modified in Version 4.1.3 (continued)*

Mode	Command and Syntax	Description
Global configuration	accelerator video	Added the overload option to the type keyword.
	disk error-handling	Removed threshold (default is 1) and reload (default is on) options.
	disk logical shutdown	Added the force keyword to the no option.
	interface GigabitEthernet	Removed the ability to specify more than one channel group or standby group; removed the priority option for standby group and added the primary option.
	interface portchannel	Removed the ability to specify more than one port channel.
	interface standby	Removed the ability to specify more than one standby interface and removed the errors option.
	port-channel	Added the src-dst-ip-port load-balancing option and removed the dst-ip option.
	snmp-server trap-source	Removed the ability to specify more than one port channel.
	virtual-blade	Changed the maximum number of virtual blades supported to six, depending on the hardware support.
Interface configuration	standby	Removed the ability to specify more than one standby group number, removed the description , errors , ip , priority , and shutdown options. Added the primary option.
Virtual blade configuration	device	Added keyboard option.

Table 3 lists commands that have been removed in WAAS version 4.1.3.

Table 3 *CLI Commands Removed in Version 4.1.3*

Mode	Command
EXEC	show standby (use show interface standby 1)

Table 4 lists commands whose names have changed in WAAS version 4.1.3.

Table 4 *CLI Commands with Changed Names in Version 4.1.3*

Mode	Old Command Name	New Command Name
EXEC	show statistics connection all	show statistics connection

Software Version 4.1.3 Monitoring API Changes

This section lists the modified and new Monitoring APIs in WAAS software version 4.1.3.

- [getMonitoredApplications](#), page 21
- [CIFSSStats](#), page 21
- [New APIs](#), page 22

getMonitoredApplications

The input parameter has been removed and the output parameter returns a list of MonitoredApps objects instead of a list of application names. The MonitoredApps object includes the application name and the monitoring status. (See [Table 5](#).)



Note

If you are using WAAS version 4.1.1 getMonitoredApplications API, you need to modify the client program before using WAAS version 4.1.3 Monitoring API.

Table 5 *MonitoredApps*

Name	Type	Description
applicationName	xs:string	Name of the Application
monitored	xs:boolean	Status of the Application that is monitored. Set to true if it is monitored and set to false if it is not monitored.

[Table 6](#) shows the getMonitoredApplications API change between WAAS versions 4.1.1 and 4.1.3.

Table 6 *getMonitoredApplications change*

Web Service	API Name	WAAS 4.1.1		WAAS 4.1.3	
		Input	Output	Input	Output
TrafficStats	getMonitoredApplications	name:string	String		MonitoredApps

CIFSSStats

The output objects of CIFSSStats web service APIs have changed. (See [Table 7](#).)



Note

If you are using WAAS version 4.1.1 CIFSSStats APIs, you need to modify the client program before using WAAS version 4.1.3 Monitoring API because the return objects have changed.

Table 7 *CIFSSStats output objects*

CIFSSStats API	Output Object (4.1.1)	Output Object (4.1.3)
retrieveCacheObjectCount	CIFSCacheCountStats	CacheCountStats
retrieveCacheUtilization	CIFSCacheUtilizationStats	CacheUtilizationStats
getCIFSCoreCount	CIFSCoreCountStats	CoreCountStats
getDiskCapacity	CIFSDiskCapacityStats	DiskCapacityStats
getOpenFileCount	CIFSFileCountStats	FileCountStats
retrieveRequestHitRate	CIFSHitRateStats	HitRateStats
getRequestCount	CIFSRequestCountStats	RequestCountStats
getOptCIFSSessionCount	CIFSSessionCountStats	SessionCountStats

Table 8 shows the CIFSSStats API output objects changes between WAAS versions 4.1.1 and 4.1.3.

Table 8 *CIFSSStats changes*

WAAS 4.1.1		WAAS 4.1.3	
CIFS API Output Object	Attributes (attribute name:data type)	CIFS API Output Object	Attributes (attribute name:data type)
CIFSCacheCountStats	inCacheCount:int outCacheCount:int timestamp:dateTime frequency:string	CacheCountStats	cachecount:int timestamp:dateTime frequency:string
CIFSCacheUtilizationStats	inCacheUtilization:int outCacheUtilization:int timestamp:dateTime frequency:string	CacheUtilizationStats	diskutilization:int resourceutilization:int timestamp:dateTime frequency:string
CIFSCoreCountStats	inCoreCount:int outCoreCount:int timestamp:dateTime frequency:string	CoreCountStats	corecount:int timestamp:dateTime frequency:string
CIFSDiskCapacityStats	inDiskCapacity:int outDiskCapacity:int timestamp:dateTime frequency:string	DiskCapacityStats	diskcapacity:int timestamp:dateTime frequency:string
CIFSFileCountStats	inFileCount:int outFileCount:int timestamp:dateTime frequency:string	FileCountStats	filecount:int timestamp:dateTime frequency:string
CIFSHitRateStats	inHitrate:int outHitrate:int timestamp:dateTime frequency:string	HitRateStats	hitrate:int timestamp:dateTime frequency:string
CIFSRequestCountStats	inRequestCount:int outRequestCount:int timestamp:dateTime frequency:string	RequestCountStats	requestcount:int timestamp:dateTime frequency:string
CIFSSessionCountStats	inSessionCount:int outSessionCount:int timestamp:dateTime frequency:string	SessionCountStats	sessioncount:int timestamp:dateTime frequency:string

New APIs

Table 9 lists the new APIs in WAAS version 4.1.3:

Table 9 **New APIs**

Web Service	API Name	Input Parameters	Output Parameters
DeviceStatus	getMonitoredAOs	name:string objType:string	MonitoredAO
	getMonitoredAOsByWaeIds	ids:long	MonitoredAO
SSLStats	getOptConnCount	name:string objType:string timeframe:TimeFrame Filter	SSLOptConnCount
	getTotalConnCount	name:string objType:string timeframe:TimeFrame Filter	SSLTotalConnCount
	getBytesCount	name:string objType:string timeframe:TimeFrame Filter	SSLBytesCount
	getUnAccelConnCount	name:string objType:string timeframe:TimeFrame Filter	SSLUnAccelConnCount
	getErrorConnCount	name:string objType:string timeframe:TimeFrame Filter	SSLErrorConnCount

Table 9 **New APIs**

Web Service	API Name	Input Parameters	Output Parameters
CIFStats	getCIFSCoreEdgeTraffic	name:string objType:string trafficType:string direction:string timeframe:TimeFrame Filter	CIFSTrafficStats
	getCIFSEdgeCoreTraffic	name:string objType:string trafficType:string direction:string timeframe:TimeFrame Filter	CIFSTrafficStats
	getCIFSClientAvgThroughput	name:string objType:string trafficType:string direction:string timeframe:TimeFrame Filter	ClientAvgThroughputStats
	getCIFSEdgeCount	name:string objType:string trafficType:string direction:string timeframe:TimeFrame Filter	EdgeCountStats

WAAS Documentation Set

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

- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*

- *Installing the Cisco WAE Inline Network Adapter*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Regulatory Compliance and Safety Information for the Cisco Content Wide Area Virtualization Engines*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[WAAS Documentation Set](#)” section.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.

