Release Note for Cisco Wide Area Application Services Software Version 5.0.1x

November 13, 2012

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

Contents

These release notes apply to the following software versions for the Cisco Wide Area Application Services (WAAS) software:

- 5.0.1

For information on WAAS features and commands, see the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

Note The WAAS Central Manager must be the highest version of all devices in your WAAS network. Upgrade the Central Manager first before upgrading any other devices.

These release notes contain the following sections:

Cisco Systems, Inc.
www.cisco.com

New and Changed Features

The following sections describe the new and changed features in software Version 5.0.1x:

Software Version 5.0.1 New and Changed Features

WAAS software Version 5.0.1 includes the following new features and changes:

- Cisco AppNav—The Cisco AppNav solution is a combination hardware and software solution that uses the new Cisco AppNav Controller Interface Modules to simplify network integration of WAN optimization and can overcome challenges with provisioning, scalability, asymmetry, and high availability. When equipped with a Cisco AppNav Controller Interface Module, a WAVE appliance can operate in the new AppNav Controller device mode where it intercepts network traffic and distributes that traffic to one or more WAAS nodes for optimization. AppNav greatly reduces dependency on the intercepting switch or router by distributing traffic among WAAS nodes for optimization using a powerful class and policy mechanism that can be configured to optimize traffic based on branch or application affinity.
- Support for three new Cisco AppNav Controller Interface Modules—12xGE copper and 12xGE SFP fiber interface modules are available for WAVE-694/7541/7571/8541 platforms and a 4x10GE SFP+ fiber interface module is available for the WAVE-594 appliance. These interface modules allow WAVE appliance operation in the new AppNav Controller device mode and support both inline and WCCP traffic interception.
- Central Manager—The WAAS Central Manager user interface has been streamlined, supports more browsers, has reorganized and easier to use menu navigation, and makes it easier to switch between devices and groups. The monitoring and reporting facility has improved graphical reports and charts and can monitor individual class maps. A new Reports Central user interface simplifies report management. A new alarm reporting panel makes alarms always accessible with one click.
- SMB Application Accelerator—A new SMB application accelerator optimizes CIFS traffic. This application accelerator supports SMBv1, has added support for native SMBv2 protocols, and optimizes signed SMBv2 traffic. (It does not provide appreciable optimization benefits for signed SMBv1 traffic.) To optimize CIFS traffic, you can choose between the CIFS and SMB application accelerators, which cannot be enabled simultaneously. The SMB accelerator does not yet support prepositioning or the Windows Print accelerator.
- Encrypted MAPI Application Acceleration—The MAPI application accelerator is enhanced to optimize encrypted MAPI traffic over secure connections using DCERPC privacy (encryption and signing).

Note The encrypted MAPI feature is in extended beta trials. You must contact waas-emapi-cs@external.cisco.com with your Cisco account team on the CC for approvals, before enabling this feature. Only approved customers will be supported for beta evaluations. The encrypted MAPI feature will be made generally available in a following release.

- SSL Application Acceleration Enhancement—The SSL application accelerator is enhanced to support Simple Certificate Enrollment Protocol (SCEP).
- Data Redundancy Elimination (DRE) Enhancements—DRE is enhanced for better performance and a new feature allows the system to bypass DRE optimization for traffic flows that do not benefit from such optimization.
- WAAS Express Support—Support for interoperability with WAAS Express in Cisco IOS Release 15.2(3)T or later. WAAS Express is enhanced with added support for HTTPS traffic as well as improved performance for file operations.
- Windows Domain Configuration Enhancements—Automatic detection of Kerberos domain settings and a simpler user interface eases Windows domain join configuration.
- Policy Enhancements—Optimization policy is simplified with a new user interface and CLI, and AppNav policy is introduced to control traffic distribution in an AppNav deployment.
- Application Accelerator Monitoring—A new application accelerator monitoring features allows you to set a load threshold that triggers an alarm if an application accelerator becomes overloaded.
- Troubleshooting Enhancements—New WAAS TCP Traceroute and AppNav connection tracing tools, and a new packet capture CLI command, provide better network and configuration troubleshooting.
- WCCP Enhancements—Enhancements include a Layer 2 egress method, a new mode to support AppNav deployments, and faster failure detection options (3 and 6 seconds) on AppNav Controllers. Additionally, WCCP flow protection is disabled by default on new installations (previously, flow protection was enabled by default, with no timeout). The Central Manager now manages WCCP configuration at the device level only; device group settings for WCCP are no longer supported but settings can be copied between devices. Static bypass lists are no longer supported on WAAS devices running WAAS version 5.0.1 or later; interception ACLs provide this functionality. WCCP configuration is simplified and the return method is set the same as the redirect method. The available egress methods also depend on the redirect method.
- Interface Configuration Enhancements—You can now designate a specific interface to handle all management traffic. Standby groups can include port-channel interfaces, and a new src-dst-ip port-channel load balancing method is available. Jumbo maximum transmission unit (MTU) frames are supported. A new bridge group type is introduced to support bridging inline interfaces on an AppNav Controller.
- AAA Enhancements—The AAA accounting facility is enhanced with the ability to enable and disable the accounting of CLI commands that result from Central Manager actions.
- SNMP Enhancements—The CISCO-APPNAV-MIB is provided to allow monitoring of AppNav deployments and the CISCO-WAN-OPTIMIZATION-MIB is enhanced to allow better monitoring of the system and individual application accelerators. Additionally, the obsolete ACTONA-ACTASTOR-MIB is removed.
- WAE-512 and WAE-612 appliances and NME-WAE-302 and NME-WAE-522 modules—These appliances and modules are no longer supported and WAAS version 5.0 and later does not operate on these appliances and modules. Upgrading to WAAS version 5.0 on these devices (or on a device group that contains any of these devices) is not allowed.
- Baseline Groups—Support for baseline groups is removed in WAAS version 5.0.
- CLI commands—For CLI command changes, see the "Software Version 5.0.1 Command Changes" section on page 22.
- Monitoring API—For API changes, see the "Software Version 5.0.1 Monitoring API Changes" section on page 27.

Software Version 5.0.1 Filenames

This section describes the WAAS software Version 5.0.1 software image files for use on WAAS appliances and modules and contains the following topics:

Standard Image Files

WAAS software Version 5.0.1 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-5.0.1.*x*-k9.bin—Universal software image that includes Central Manager, Application Accelerator, and AppNav Controller functionality. You can use this type of software file to upgrade a device operating in any device mode.
- waas-accelerator-5.0.1.*x*-k9.bin—Application Accelerator software image that includes Application Accelerator and AppNav Controller functionality only. You can use this type of software file to upgrade only an Application Accelerator or AppNav Controller device. 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-5.0.1.*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-5.0.1.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-5.0.1.*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-5.0.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.0.1.*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-5.0.1.*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 5.0.1 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-5.0.1.*x*-npe-k9.bin—Universal NPE software image that includes Central Manager, Application Accelerator, and AppNav Controller functionality. You can use this type of software file to upgrade a device operating in any device mode.

- waas-accelerator-5.0.1.*x*-npe-k9.bin—Application Accelerator NPE software image that includes Application Accelerator and AppNav Controller functionality only. You can use this type of software file to upgrade only an Application Accelerator or AppNav Controller device. 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-5.0.1.*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-5.0.1.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-5.0.1.*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-5.0.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.0.1.*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-5.0.1.*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.)

WAAS Appliance System Firmware Update

On WAE and WAVE appliances, we recommend that you update the following three types of system firmware to the latest version, to best support new WAAS features:

- BIOS on the WAVE-594/694/7541/7571/8541 models—For details, see the "BIOS Update" section on page 5. The latest BIOS is required for AppNav operation.
- BMC firmware on the WAVE-294/594/694/7541/7571/8541 models—For details, see the "BMC Firmware Update" section on page 6. The latest BMC firmware is required for the IPMI over LAN feature.
- RAID controller firmware on the WAE-674/7341/7371 and WAVE-7541/7571/8541—For details, see the "RAID Controller Firmware Update" section on page 7. The latest RAID controller firmware is recommended to avoid some rarely encountered RAID controller issues.

BIOS Update

The latest BIOS is required for AppNav operation with a Cisco AppNav Controller Interface Module in WAVE-594/694/7541/7571/8541 models. WAVE-294 models do not need a BIOS update.

WAAS appliances shipped from the factory with WAAS version 5.0.1 or later have the correct BIOS installed. If you are updating a device that was shipped with an earlier version of WAAS software, you should update the BIOS, unless it was updated previously. WAVE-594/694 models require BIOS version 17A and WAVE-7541/7571/8541 models require BIOS version 11A.

If you install a Cisco AppNav Controller Interface Module in a device that requires a BIOS update, the bios_support_seiom major alarm is raised, "I/O module may not get the best I/O performance with the installed version of the system BIOS firmware."

To determine if a device has the correct BIOS version, use the **show hardware** command. The following example displays the BIOS version installed on the device, which is the last three digits of the Version value:

```
wave# show hardware
...
WAVE-594-K9

BIOS Information:
Vendor          :American Megatrends Inc.
Version         :A31C117A                          <<<<< version 17A
Rel. Date       :02/24/2012
...
```

If a BMC firmware update is needed, you can download it from cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image is named waas-bios-installer-16a-17a-11a-k9.bin.

You can use the following command to update the BIOS from the image file that is available through FTP on your network:

copy ftp install *ip-address remotefiledir* **waas-bios-installer-16a-17a-11a-k9.bin**

The complete update process can take several minutes and the device may appear unresponsive but do not interrupt the process or power cycle the device. After the update is complete, you must reload the device.

After the device reboots, you can verify the firmware version by using the **show hardware** command.

BMC Firmware Update

IPMI over LAN requires that you install a specific BMC firmware version on the device. The minimum supported BMC firmware versions are as follows:

- WAVE-294/594/694—48a
- WAVE-7541/7571/8541—26a

WAAS appliances shipped from the factory with WAAS version 4.4.5 or later have the correct firmware installed. If you are updating a device that was shipped with an earlier version of WAAS software, you must update the BMC firmware, unless it was updated previously.

To determine if you are running the correct firmware version, use the **show bmc info** command. The following example displays the latest BMC firmware version installed on the device (48a here):

```
wave# show bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.48                    <<<<< version 48
IPMI Version              : 2.0
Manufacturer ID           : 5771
Manufacturer Name         : Unknown (0x168B)
Product ID                : 160 (0x00a0)
Product Name              : Unknown (0xA0)
Device Available          : yes
Provides Device SDRs      : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info     :
    0x0b
```

```
    0x0c
    0x08
    0x0a                                          <<<<< a
. . .
```

If a BMC firmware update is needed, you can download it from cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image is named waas-bmc-installer-48a-48a-26a-k9.bin.

You can use the following command to update the firmware from the image file that is available through FTP on your network:

copy ftp install *ip-address remotefiledir* **waas-bmc-installer-48a-48a-26a-k9.bin**

The update process automatically checks the health status of the BMC firmware. If the system detects that the BMC firmware is corrupted, BMC is recovered during the BMC firmware update procedure. The complete update process can take several minutes. If the device appears unresponsive, do not interrupt the process or power cycle the device. After the update is complete, you must reload the device.

After the device reboots, you can verify the firmware version by using the **show bmc info** command.

BMC recovery and BMC firmware update restores the factory defaults on the BMC and all the current IPMI over LAN configurations are erased.

If the BMC firmware gets corrupted, a critical alarm is raised.

RAID Controller Firmware Update

We recommend that you upgrade to the latest RAID controller firmware for your hardware platform, which can be found on cisco.com at the Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware differs depending on your hardware platform:

- WAVE-7541/7571/8541—Update to the 12.12.0 (0060) RAID Controller Firmware (or later version).

  The firmware binary image is named waas-raid-fw-installer-12.12.0-0060-k9.bin. Instructions on how to apply the firmware update are posted on cisco.com together with the firmware in the file named M2_0060_FIRMWARE.pdf, which you can see when you mouse over the firmware file.

- WAE-674/7341/7371—Update to the 5.2-0 (17002) RAID Controller Firmware (or later version). You can check your current RAID controller firmware version with the **show disk tech-support** EXEC command. The Firmware field displays the firmware version.

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

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 file cannot be generated and copied to /local/local1.

  Both 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, which indicates 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 (17002) RAID Controller Firmware (or later version).

Upgrading and Interoperability

This section contains the following topics:

Interoperability and Support

Table 1-1 lists the hardware, client, and web browser support for WAAS software version 5.0.1.

Table 1-1 Hardware, CIFS Client, Web Browser Support

Hardware support	The WAAS software operates on these hardware platforms: WAE-674, WAE-7341, WAE-7371, WAVE-274, WAVE-474, WAVE-574, WAVE-294, WAVE-594, WAVE-694, WAVE-7541, WAVE-7571, or WAVE-8541 appliance, or an NME-WAE-502, SM-SRE-700, SM-SRE-710, SM-SRE-900, or SM-SRE-910 network module that is installed in specific Cisco routers. Additionally, Cisco 880 Series, 890 Series, and ISR G2 routers running WAAS Express are supported on the branch side (WAAS version 4.2.1 or later is required on the data center side). You must deploy the WAAS Central Manager on a dedicated device.
CIFS client support	The WAAS software running on a branch WAE interoperates with these CIFS clients: Windows 98/NT 4.0/2000/XP/Vista/7 and Windows Server 2003/2008 R2.
Web browser support	The WAAS Central Manager GUI requires Internet Explorer version 8 or 9 (only 8 on Windows XP), Firefox version 4 or later, Chrome version 10 or later, or Safari version 5.x (only on Apple OS X) and the Adobe Flash Player browser plug-in. The WAE Device Manager GUI requires Internet Explorer version 5.5 or later.

If you are using Internet Explorer to access the Central Manager GUI, we strongly recommend that you install the Google Chrome Frame plug-in to provide better performance. When you log into the Central Manager the first time, you are prompted to install Google Chrome Frame. Choose a language, click **Get Google Chrome Frame**, and follow the prompts to download and install the plug-in. If you do not want to install the plug-in, click the link to continue without installing Google Chrome Frame.

Note When using Internet Explorer, ensure that the Tools > Internet Options > Advanced tab > Do not save encrypted pages to disk check box (under Security) is checked. If this box is unchecked, some charts do not display (CIFS device level charts and version 4.x scheduled reports that have completed).

WAAS Version Interoperability

Consider the following guidelines when operating a WAAS network that mixes Version 5.0.x devices with devices running earlier software versions:

- WAAS Version 5.0.x is not supported running in a mixed version WAAS network where any WAAS device is running a software version earlier than 4.2.1. If you have any WAAS devices running a version earlier than 4.2.1, you must first upgrade them to Version 4.2.1 (or a later version) before you install Version 5.0. Do not upgrade any device to a version later than the existing Central Manager version. After all devices and the Central Manager are running version 4.2.1 or later, you can begin the upgrade to version 5.0.1 on the WAAS Central Manager. Directly upgrading a device from version 4.0 or 4.1 to 5.0 is not supported.
- In a mixed version WAAS network, the WAAS Central Manager must be running the highest version of the WAAS software.

AppNav Interoperability

Consider the following guidelines when deploying the Cisco AppNav solution:

- If you are connecting an AppNav Controller (ANC) to a Catalyst 6500 series switch and you have configured the ANC to use WCCP with the L2 redirect method, do not deploy the ANC on the same subnet as the client computers. This configuration can cause packet loss due to a limitation of the Catalyst 6500 series switch.
- All WAAS nodes in an AppNav deployment must be running WAAS version 5.0 or later.
- WAAS Express devices cannot operate as WAAS nodes in an AppNav deployment.

WAAS Express Interoperability

Consider the following guideline when using WAAS Express devices in your WAAS network:

- When using a WAAS device running version 5.0 and a WAAS Express peer device running Cisco IOS Release 15.2(2)T or earlier, connections originating from the WAAS device and sent to the WAAS Express peer are passed through instead of being optimized. We recommend upgrading to WAAS Express in Cisco IOS Release 15.2(3)T or later to take advantage of the latest enhancements.

WCCP Interoperability and Upgrade

Central Managers running Version 5.0.1x can manage WAEs running software Versions 4.2.1 and later. However, we recommend that all WAEs in a given WCCP service group be running the same version.

Note All WAEs in a WCCP service group must have the same mask, redirect, and return methods. If an upgrade causes these values to change, upgraded WAEs are not able to rejoin the service group until all WAEs in the group are upgraded.

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 **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.

Step 5 Ensure that all WAEs in the service group are using the same redirect and return methods. If you are upgrading from version 4.x to 5.x, the return method is no longer configurable and is set the same as the redirect method. If you had been using a redirect method of L2 and a return method of GRE, this is no longer supported and the return method is changed to L2 after the upgrade. Ensure that your router software supports L2 return. If it does not, you can change your redirect method to GRE, which causes the return method to change to GRE.

Step 6 Reenable 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
```

Upgrading from a Prerelease Version to Version 5.0.1x

To upgrade from WAAS prerelease software to Version 5.0.1x, 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 or USB flash drive.

Upgrading from a Release Version to Version 5.0.1x

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 5.0.1x, observe the following guidelines and requirements:

- Upgrading to Version 5.0.1 is supported only from Versions 4.2.1, 4.2.3, 4.2.3b, 4.2.3c, 4.3.1, 4.3.3, 4.3.5a, 4.4.1, 4.4.3, 4.4.3a, 4.4.3b, 4.4.3c, 4.4.5, 4.4.7, and 4.5.1. 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 5.0.1 version.

- Upgrading to Version 5.x is not supported on the following platforms: WAE-511, WAE-512, WAE-611, WAE-612, WAE-7326, NME-WAE-302, and NME-WAE-522. WAAS Version 5.x does not operate on these appliances. Upgrading a device group is not allowed if the group contains any of the unsupported devices. If you have a Central Manager running on one of these unsupported platforms, you can migrate it to a supported platform by following the procedure in the "Migrating a Central Manager from an Unsupported Platform" section on page 14.
- 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 and no WAAS device should be running a version earlier than version 4.2.1.
- 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 a WAAS Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.
- Before upgrading a WAAS Central Manager to Version 5.0.1, make a database backup by using the **cms database backup** EXEC command. Use the **copy disk ftp** EXEC command to move the backup file to an external system. In case of any problem during the upgrade, you can restore the database backup that you made before upgrading by using the **cms database restore** *backup-file* EXEC command, where *backup-file* is the one created by the **backup** command.
- After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If any of the application accelerators were enabled on the device before the upgrade, you should enable the Enterprise license. 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 class maps are configured. For more information on configuring accelerators, policies, and class maps, see the "Configuring Application Acceleration" chapter in the *Cisco Wide Area Application Services Configuration Guide*.
- If you are upgrading a WAAS Central Manager from a version earlier than 4.4.1 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 > Security > Secure Store** or use the **cms secure-store open** EXEC command. After upgrading, 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 5.0.1, 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 5.0.1, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you are upgrading a Central Manager from Version 4.2.3x or earlier, and you have any scheduled reports that are configured for more than 100 recurrences, only 100 recurrences are retained after the upgrade.

- If you use the setup utility for basic configuration after upgrading to 5.0.1, 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 5.0.1 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 5.0.1 (non-NPE).
- 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.
- Beginning with Version 4.4.1, application-aware DRE changed the way the DRE cache is populated and managed. When upgrading 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. DRE on a Version 5.x device is compatible with all Version 4.1.x, 4.2.x, 4.3.x, 4.4.x, and 4.5.x peers but is not compatible with 4.0.x peers.

  Application policies do not change, but the new “bidirectional” term is introduced, which is the mode used prior to Version 4.4.1.
- After upgrading WAAS accelerator devices from a version earlier than 4.4.1, you may be able to improve DRE disk performance by deleting and recreating disk data partitions by using the **disk delete-data-partitions** EXEC command. This command deletes the DRE and CIFS caches and all installed virtual blade images. If you want to keep virtual blade images, back them up before using this command by using the **copy virtual-blade** EXEC command.

  After using the **disk delete-data-partitions** command, you must reload the device and the data partitions are automatically recreated and the caches are initialized, which can take several minutes. DRE optimization is not done until the DRE cache has finished initializing. The **show statistics dre** EXEC command reports “TFO: Initializing disk cache” until then.
- When upgrading a WAAS accelerator device from a version earlier than 4.4.1, the WCCP load-balancing assignment method is always strictly enforced and must match the farm assignment method or the WAAS device is not allowed to join the farm. Nonstrict assignment method is no longer an option.

  When upgrading a Central Manager from a version earlier than 4.4.1, the Only Use Selected Assignment Method check box is no longer available in the device group WCCP Settings window. Any WAEs in a device group that are running a version earlier than 4.4.1 and getting their WCCP settings from the device group will not use strict assignment method enforcement. This does not affect the WCCP farm.
- The method for associating virtual blade interfaces to physical interfaces changed in Version 4.4.1 to use bridge groups and Bridge Virtual Interfaces (BVIs). When upgrading a device with a virtual blade from a version earlier than 4.4.1, any virtual interface configurations are converted to use the new bridging method.
- Legacy mode WAFS is no longer supported in Version 4.4.1 or later and upgrading 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 or later. On upgrading from a version earlier than 4.4.1, legacy print services functionality is removed and users must use the Windows Print accelerator. The print role and print admin privileges are removed from all user accounts, and the functionality of the Central Manager acting as a print repository is removed. Any legacy print services jobs that are spooled are lost if an upgrade is done before the data is printed.

A Version 4.4.1 or 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.

- In WAAS versions before 4.4.5, you were able to configure more memory for virtual blades on a 294-4G platform than was supported for virtual blades. To maintain stability, after upgrading from a version earlier than 4.4.5, all memory allocated to virtual blades on the 294-4G platform is limited to 1 GB. This change affects any existing 294-4G virtual blade configurations.
- Version 5.0 no longer supports device group configuration of the following features: static bypass lists, vPath interception, and WCCP. When you are upgrading to version 5.0 from a previous version, any device group configurations of these features are copied to the individual devices and the device group settings are removed. WCCP settings can be copied between devices.
- The default WCCP return method changed in WAAS version 5.0. If you are upgrading from version 4.x to 5.x, the return method is no longer configurable and is set the same as the redirect method. If you had been using a redirect method of L2 and a return method of GRE, this is no longer supported and the return method is changed to L2 after the upgrade. Ensure that your router software supports L2 return. If it does not, you can change your redirect method to GRE, which sets the return method to GRE.
- The default WCCP egress method changed in WAAS version 5.0 and the redirect method determines the default and available egress methods. For L2 redirect, the default egress method is set to Layer 2 and an alternate option is IP forwarding. For GRE redirect, the default egress method is IP forwarding, and alternate options are WCCP GRE and generic GRE.
- When upgrading from a WAAS version earlier than 5.0, you must rename classifier names that contain a period (.) to remove the period. Classifiers with a period in their name are deleted on an upgrade. Replace periods in classifiers with a hyphen (-) or underscore (_) to prevent deletion.
- When upgrading from a WAAS version earlier than 5.0, pending reports are carried forward. Charts in reports are retained if they are still available; if they are no longer available, they are migrated to new charts. Any duplicated charts (as a result of migration) in a report are removed and all ICA application accelerator reports are removed because they are all new in version 5.0. Custom reports are migrated to new custom reports in a similar way. Completed reports from before the upgrade are shown in the Completed Reports list and maintain their original format.
- When upgrading from a WAAS version earlier than 5.0, classifiers and policies are migrated to new version 5.0 class maps and policy rules. The same functionality is maintained, though the class map and policy framework is different.
- When upgrading a Central Manager from a WAAS version earlier than 5.0, the WAFS application definition is migrated to a new CIFS application, except if a CIFS application already exists, the application name change is not done. If you upgrade a WAE device that is not registered to a Central Manager, the WAFS application is not renamed. Any WAAS device that is still using the WAFS application in a policy rule after an upgrade to version 5.0 raises the following alarm: “WAFS application is configured for optimization. Consider changing the application name to CIFS.” To clear the alarm, you can manually change the policy rule to use the CIFS application or restore default policies.

- When upgrading from WAAS version 4.5 to version 5.0, the ICA classifiers are automatically changed from ica and citriximaclient to class maps named Citrix-ICA and Citrix-CGP, respectively. They are also moved to a new application named Citrix. There is no difference in functionality.

  The ICA charts in WAAS version 5.0 and later are also different from those used in version 4.5. If you are viewing the data from a version 4.5 WAAS device, the charts appear empty due to the different data that the device is collecting. The ICA data for version 4.5 WAAS devices is available in the system level TCP Summary Report by selecting the Remote-Desktop application.
- When you upgrade from WAAS, version 4.x, you must reconfigure the custom EPM policy for a device or device group. You must first restore the default policy setting by selecting the **Restore default Optimization Policies** link for the device group in the Modifying Device Group window and then reconfigure your custom policy rules for the device.

Migrating a Central Manager from an Unsupported Platform

If you have a WAAS Central Manager that is running on a hardware platform that is unsupported in version 5.0 (such as a WAE-511/512/611/612/7326), you are not allowed to upgrade the device to version 5.0. You must migrate the Central Manager to a supported platform by following the procedure in this section, which preserves all of the Central Manager configuration and database information.

Follow these steps to migrate a primary Central Manager to a new WAAS device:

Step 1 From the primary Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device by using the **copy disk ftp** command.

```
CM# cms database backup
Creating database backup file cms-db-06-28-2012-15-08_5.0.1.0.15.dump
Backup file cms-db-06-28-2012-15-08_5.0.1.0.15 is ready.
Please use `copy' commands to move the backup file to a remote host.
CM# copy disk ftp 10.11.5.5 / cm-backup.dump cms-db-06-28-2012-15-08_5.0.1.0.15.dump
```

Step 2 Display and write down the IP address and netmask of the Central Manager.

```
CM# show running-config interface
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.10.10.25 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
```

Step 3 Shut down all the interfaces on the primary Central Manager.

```
CM# configure
CM(config) interface GigabitEthernet 1/0 shutdown
```

Step 4 Replace the existing Central Manager device with a new hardware platform that can support WAAS version 5.0. Ensure that the new Central Manager device is running the same software version as the old Central Manager.

Step 5 Configure the new Central Manager with the same IP address and netmask as the old Central Manager. You can do this in the setup utility or by using the **interface** global configuration command.

```
newCM# configure
newCM(config) interface GigabitEthernet 1/0 ip address 10.10.10.25 255.255.255.0
```

Step 6 Copy the backup file created in Step 1 from the FTP server to the new Central Manager.

```
newCM# copy ftp disk 10.11.5.5 / cm-backup.dump cms-db-06-28-2012-15-08_5.0.1.0.15.dump
```

Step 7 Restore the database backup on the new Central Manager by using the **cms database restore** command. Use option 1 to restore all CLI configurations.

```
newCM# cms database restore cms-db-06-28-2012-15-08_5.0.1.0.15.dump
Backup database version is from an earlier version than the current software version.
Restored data will be automatically upgraded when cms services are enabled.
Restoring the backed up data. Secure-Store will be re-initialized.
Successfully migrated key store
***** WARNING : If Central Manager device is reloaded, you must reopen Secure Store with
the correct passphrase. Otherwise Disk encryption, CIFS preposition, SSL, AAA and other
secure store dependent features may not operate properly on WAE(s).*****
Successfully restored secure-store. Secure-store is initialized and opened.
Overwrite current key manager configuration/state with one in backup (yes|no) [no]?yes
Restoring CLI running configuration to the state when the backup was made. Choose type of
restoration.
1. Fully restore all CLI configurations.
2. Partially restore CLI configurations, omitting network configuration settings.
3. Do not restore any CLI configurations from the backup.
Please enter your choice : [2] 1
Please enable the cms process using the command 'cms enable' to complete the cms database
restore procedure.
Database files and node identity information successfully restored from file
`cms-db-06-28-2012-15-08_5.0.1.0.15.dump'
```

Step 8 Enable the CMS service.

```
newCM# configure
newCM(config) cms enable
```

Step 9 Verify that the Central Manager GUI is accessible and all WAAS devices are shown in an online state in the Devices window.

Step 10 (Optional) If you have a standby Central Manager that is running on unsupported hardware and is registered to the primary Central Manager, deregister the standby Central Manager.

```
standbyCM# cms deregister
```

Step 11 Upgrade the primary Central Manager to WAAS version 5.0.x. You can use the Central Manager Software Update window or the **copy ftp install** command.

Step 12 Verify that the Central Manager GUI is accessible and all WAAS devices are shown in an online state in the Devices window.

Step 13 (Optional) Register a new standby Central Manager that is running WAAS version 5.0.x.

```
newstandbyCM# configure
newstandbyCM(config)# device mode central-manager
newstandbyCM(config)# exit
newstandbyCM# reload
...
```

Wait for the device to reload.

```
newstandbyCM# configure
newstandbyCM(config)# central-manager role standby
newstandbyCM(config)# central-manager address 10.10.10.25
newstandbyCM(config)# cms enable
```

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 5.0.1x to a Previous Version

Note the following guidelines and considerations for downgrading:

- Downgrade is supported only to versions 4.2.1, 4.2.3, 4.2.3b, 4.2.3c, 4.3.1, 4.3.3, 4.3.5a, 4.4.1, 4.4.3, 4.4.3a, 4.4.3b, 4.4.3c, 4.4.5, 4.4.7, and 4.5.1. Downgrade is not supported to versions 4.1.x and 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 Central Manager (if you have one), and lastly the primary Central Manager.
- If you have a standby Central Manager, it must be registered to the primary Central Manager before the downgrade.
- When downgrading an AppNav Controller device to a version earlier than 5.0.1 you must deregister the device from the Central Manager, change the device mode to application-accelerator, downgrade the device, and then reregister the device after the downgrade (or you can reregister the device before downgrading). If you do not deregister the device before downgrading, the device goes offline and the device mode is not set correctly. In that case, use the **cms deregister force** EXEC command to deregister the device and then reregister it by using the **cms enable** global configuration command.

  If the AppNav Controller device contains an AppNav Controller Interface Module, the module is not recognized by WAAS versions earlier than 5.0.1 and is nonfunctional after a 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 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.
- Locked-out user accounts are reset upon a downgrade.
- Any reports and charts that are not supported in the downgrade version are removed from managed and scheduled reports when you downgrade to an earlier version. Any pending reports that were carried forward from an upgrade from a version earlier than 5.0 are maintained.
- 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.
- Current BMC settings are erased and restored to factory-default when you downgrade WAAS to a version earlier than 4.4.5.

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 by using the **copy disk ftp** command.

```
CM# cms database backup
Creating database backup file cms-db-06-28-2012-15-08_5.0.1.0.15.dump
Backup file cms-db-06-28-2012-15-08_5.0.1.0.15 is ready.
Please use `copy' commands to move the backup file to a remote host.
CM# copy disk ftp 10.11.5.5 / 06-28-backup.dump cms-db-06-28-2012-15-08_5.0.1.0.15.dump
```

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

```
CM# copy ftp install 10.11.5.5 waas/4.4 waas-universal-4.4.5c.4-k9.bin
```

Step 3 Reload the device.

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

Cisco WAE and WAVE Appliance Boot Process

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

Cisco WAE and WAVE appliances may 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.

Operating Considerations

This section includes operating considerations that apply to software Version 5.0.1x and contains the following topics:

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.

Using Autoregistration with Port-Channel and Standby Interfaces

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

Disabling WCCP from the Central Manager

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

Changing Device Mode To or From Central Manager Mode

If you change the device mode to or from Central Manager mode, the DRE cache is erased.

TACACS+ Authentication and Default User Roles

If you are using TACACS+ authentication we recommend that you do not assign any roles to the default user ID, which has no roles assigned by default. If you assign any roles to the default user, external users that are authenticated by TACACS+ and who do not have the waas_rbac_groups attribute defined in TACACS+ (meaning they are not assigned to any group) can gain access to all the roles that are assigned to the default user.

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 5.0.1 Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, command changes, and monitoring API changes in software Version 5.0.1 and contains the following topics:

Software Version 5.0.1 Resolved Caveats

The following caveats were resolved in software Version 5.0.1.

Caveat ID Number	Description
CSCti33717	TCP checksum errors /Optimization fails with vmxnet3 driver and SDP
CSCtk55351	Rarely, http-ao delays handing of Connect request
CSCtl74173	WAE doesnt allow to log in via tacacs without sysfs
CSCtl87010	CifsAO is disabled when primary interface is not configured
CSCtn26093	Restore factory-default disables Auto-registration
CSCto62419	Accounting info from WAE on ACS 5.1 displays privilege 0 for Superuser
CSCto74161	Watchdog alarm may be reported after WAE reboot
CSCto75031	Race condition causing periodic remote user cleanup failure in CM logs
CSCto88400	In rare cases, box may become unresponsive following clock change
CSCtq47417	Alarm generated for CIFS AO down with misconfig Primary Interface
CSCtq54882	Preposition task may work incorrectly if eth0,eth1,fa0,fa1 are down
CSCtr42968	Manage devices page does not display list of devices
CSCtt02446	WAAS - IP ACL re-ordering issue - mapping only well known ports
CSCtt04124	KM logs shouldn't be allowed to fill up SYSFS
CSCtt04395	Certain updates sent from CM are not written to pcm config
CSCtt17284	standby CM OutofMem due to growing ao_stats_collection_info table
CSCtu02748	WAAS: Java core created in Device Manager
CSCtu15875	MAPI AO encounters keepalive issue and reloads
CSCtw62804	Device and DG level: Apply defaults button + submit returns an error
CSCtw66559	winbindd causes 100% CPU load on WAAS
CSCtw69937	Unable to set power-on operation on some WAVE platforms
CSCtx08202	TACACS authenticated CM GUI users are configured in remote devices
CSCtx10049	Fast offline detection may take time more than expected
CSCtx12835	Datamaster core file created
CSCtx27549	Slow CIFS performance due to connections not terminated appropriately
CSCtx27970	WAAS CIFS error when server sending a NT notify after a NT Cancel
CSCtx34925	WAAS preposition job will fail with internal error
CSCty17279	WAAS - Password displayed in some output as a one-way hash
CSCty68115	WAVE-75xx device-id and mac-address difference affects CM reporting
CSCty72231	Virtual Blade Crash on vnc connection
CSCty92232	Primary WAAS Central manager can become unresponsive
CSCty92233	CMS can remove local running and startup configurations

Caveat ID Number	Description
CSCtz41111	Security Web-Application-Filter TACACS SSH / console unresponsive WAAS
CSCtz45783	Log files & KDB core file got deleted by system after recovery from KDB
CSCua50771	Role does not work properly when WAAS device is accessed via PeerID link

Software Version 5.0.1 Open Caveats

The following open caveats apply to software Version 5.0.1.

Caveat ID Number	Description
CSCsi65522	CIFS related statistics graphs are not populated
CSCtd70016	Under rare circumstances, CIFS AO can not be re-enabled
CSCtk74707	Wrong Time under Connection Monitoring for WAE in CM
CSCts11444	SMBv1_0 Sessions Optimized counters are incremented incorrectly
CSCts56258	Unable to open file through CIFS AO under rare timing oplock break case
CSCtu24846	Mixed AO tests: fb_hashtbl_delete Attempted to delete a filetring tuple
CSCtu55542	ICA: XD5- word App sessions comp ratio degraded severely after few hours
CSCtx55758	packet-capture CLI fails to account for WCCP GRE
CSCty14254	Standby Interface failover to primary not sendng gratuitous ARP
CSCty23363	SMBAO: SMB connection reset during stress testing on 674
CSCty50241	OCSP request fails with bad aosh op exception
CSCtz13223	WAAS CIFS AO will produce a java hprof for scanning tool SMB request
CSCtz24645	ICA: Sever lag seen while typing text and playing a video for 300 conn
CSCtz32749	Under rare circumstances, Can not start CifsAO
CSCtz41111	Security Web-Application-Filter TACACS SSH / console unresponsive WAAS
CSCtz50283	CIFS AO may restart when reading directory with many subdirectories
CSCtz74336	WAN secure AO Callback along with dropped MAPI conenctions
CSCtz78575	HTTP-AO prevents FIN flag reaching the client
CSCtz79950	Detected TX hung issue with no device access
CSCtz88400	ERROR thrown while accessing share from Win7 to Win2k8 server
CSCtz92491	Config state is showing disabled even if SMB ao is operational.
CSCua26516	All WAE devices may appear offline in Central Manager
CSCua38244	IE crashes on clicking telnet, with google chrome frame plugin installed
CSCua55674	Changes to not to render M&R Charts with insufficient data in few cases
CSCua64085	WaasExp device group policies goes into override mode upon downgrade
CSCua64691	Launch of NAM UI failed from CM gui in IE8 with chrome frame work.
CSCua71669	In cluster wizard custom flow interface editing may fail on IE 8
CSCub69438	WAAS HTTP AO TCP re-used will mark incorrect checksums when core is 674.

Software Version 5.0.1 Command Changes

This section lists the new and modified commands in WAAS software version 5.0.1.

Table 2 lists the commands and options that have been added in WAAS version 5.0.1.

Table 2 CLI Commands Added in Version 5.0.1

Mode	Command	Description
EXEC	**clear cifs**	Clears the list of message signing servers.
	clear connection	Resets one or more connections.
	clear dre	Clears DRE configurations.
	clear service-policy	Clears AppNav and optimization class and policy map counters.
	clear statistics monitor appnav-controller traffic	Clears AppNav Controller traffic monitoring statistics.
	clear windows-domain	Clears Windows domain server information.
	copy monitoring-log	Copies SMB statistics data to the local disk or FTP server.
	debug appnav-controller connection	Enables connection debugging on an AppNav Controller.
	debug cmm	Configures cluster membership manager debugging.
	debug controllers	Configures interface controller capture debugging.
	debug encryption-service	Configures encryption service debugging.
	debug fda	Configures flow distribution agent service debugging.
	debug fdm	Configures flow distribution manager service debugging.
	debug imd	Configures interface manager debugging.
	debug nplogd	Configures NP log daemon debugging.
	debug punt	Configures punt handler debugging.
	debug rmd	Configures route manager debugging.
	debug service-insertion	Configures service-insertion module debugging.
	debug service-policy	Configures service policy debugging.
	monitor appnav-controller traffic	Enables traffic monitoring on an AppNav Controller.
	packet-capture	Captures packets.
	show appnav-controller flow-distribution	Displays ANC flow distribution information.
	show bridge	Displays bridge interface information.
	show class-map	Displays the optimization or AppNav class maps.
	show dre	Displays DRE configuration information.
	show interception-method	Displays the interception method.
	show monitor	Displays the status of traffic monitoring on an AppNav Controller.
	show policy-map	Displays the optimization or AppNav policy map rules.
	show policy-sub-class	Displays the AppNav policy subclasses.

Table 2 CLI Commands Added in Version 5.0.1 (continued)

Mode	Command	Description
	show service-insertion	Displays information about the AppNav controller configuration.
	show service-policy	Displays optimization or AppNav policy information.
	show statistics appnav-controller	Displays statistics for an AppNav Controller.
	show statistics class-default	Displays statistics information about the class-default class map.
	show statistics class-map	Displays statistics information about class maps.
	show statistics monitor appnav-controller traffic	Displays AppNav Controller traffic monitoring statistics.
	show statistics policy-sub-class	Displays the statistics for an AppNav class map.
	show statistics punt	Displays the punt statistics.
	show statistics service-insertion	Displays service context statistics.
	show statistics sessions	Displays the dynamic match session statistics.
	waas-tcptrace	Lists WAAS devices in the path to a destination host.
Global configuration	**accelerator ica**	Enables the ICA application accelerator.
	accelerator smb	Configures the SMB application accelerator.
	class-map	Configures optimization and AppNav class maps.
	dre	Enables and configures DRE auto bypass and load monitor settings.
	interception-method	Sets the traffic interception method.
	policy-map	Configures optimization and AppNav policy maps.
	service-insertion	Configures AppNav controller entities.
	service-policy	Configures AppNav and optimization policy.
	stats-collector logging	Configures SMB statistics logging.
	system jumbomtu	Configures a jumbo MTU on all interfaces.
	threshold-monitor	Configures monitoring thresholds in an AppNav deployment.
Interface configuration	**load-interval**	Configures the statistics polling interval for an interface.
WCCP configuration	**assignment-method**	Configures WCCP settings.
	egress-method	
	enable	
	exit	
	failure-detect	
	password	
	redirect-method	
	router-list-num	
	weight	

Table 2 CLI Commands Added in Version 5.0.1 (continued)

Mode	Command	Description
Service Node configuration	**authentication**	Configures WNs in an ANC Cluster.
	description	
	enable	
	shutdown	
Service Node Group configuration	**description**	Configures WNGs in an ANC Cluster.
	service-node	
Service Controller Group configuration	**description**	Configures the ANCG in an AppNav Cluster.
	appnav-controller	
Service Context configuration	**authentication**	Configures the service context in an AppNav Cluster.
	description	
	enable	
	appnav-controller-group	
	service-node-group	
	service-policy	
Class Map configuration	**description**	Configures optimization and AppNav class maps.
	match peer	
	match protocol	
	match tcp	
Policy Map configuration	**class**	Configures optimization and AppNav policy maps.
	description	
Policy Map Class configuration	**distribute**	Configures a service policy in optimization and AppNav policy maps.
	monitor-load	
	optimize	
	pass-through	
	service-policy	
	set ip dscp	

Table 3 lists existing commands that have been modified in WAAS version 5.0.1.

Table 3 CLI Commands Modified in Version 5.0.1

Mode	Command	Description
EXEC	**clear statistics**	Added **appnav-controller**, **class-map**, **punt**, and **service-insertion** options.
	debug accelerator	Added **smb** option.
	debug statistics	Added **client**, **collector**, **serializer**, and **sqm** options; removed **scheduler** option.
	ping	Added **management** option.
	show accelerator	Added **ica**, **smb**, and **wansecure** options.
	show auto-discovery	Added **asymmetric-connections** option.
	show cifs	Added **msg-signing-servers** option.
	show interface	Output changed.
	show ip access-list	Output changed for ANCs.
	show ip routes	Added **data** and **management** options.
	show statistics accelerator	Added **ica**, **smb**, and **wansecure** options.
	show statistics application	Output changed.
	show statistics connection optimized	Added **ica**, **smb**, and **wansecure** options.
	show wccp	Options and output changed.
	show wccp gre	Changed to the **show wccp statistics** command.
	show wccp wide-area-engine	Changed to the **show wccp clients** command.
	ssh	Added **management** option.
	telnet	Added **management** option.
	traceroute	Added **management** option.
	windows-domain	Added the **join** and **leave** options.

Table 3 CLI Commands Modified in Version 5.0.1 (continued)

Mode	Command	Description
Global configuration	**aaa accounting**	Added the **cms enable tacacs+** option.
	accelerator mapi	Added the **encryption** and **wansecure-mode** options.
	bridge	Added new options for inline bridge groups on AppNav controllers.
	device mode	Added **appnav-controller** option.
	inline	Removed the **enable** option. Use the **interception-method** command to enable inline mode.
	interception	Added **appnav-controller** option to configure AppNav controller access lists.
	interface bvi	Added **load-interval** option.
	interface GigabitEthernet	Added **load-interval** option.
	interface InlineGroup	Added **load-interval** option.
	interface port-channel	Added **load-interval** and **standby** options.
	interface standby	Added **load-interval** option.
	interface TenGigabitEthernet	Added **load-interval** option.
	ip	Added the **management**, **ftp**, **tftp** options.
	kerberos	Added the **dns** option.
	port-channel	Added the **src-dst-ip** option.
	primary-interface	Added the **management** option.
	transaction-logs	Added the **management** option.
	wccp flow-redirect	Added the **timeout** option and changed the default to disable flow protection for new installations.
	wccp tcp-promiscuous service-pair	Removed all options except for **service-pair**. Now enters WCCP configuration mode. All WCCP configuration commands are entered in WCCP configuration mode.
	windows-domain	Added **encryption-service** option.
Extended ACL configuration	**deny**	Added the cmm keyword as a valid UDP protocol.

Table 4 lists the commands and options that have been removed in WAAS version 5.0.1.

Table 4 CLI Commands Removed in Version 5.0.1

Mode	Command	Description
EXEC	**debug policy-engine**	Replaced by the **debug service-policy** command.
	show bypass	Displays static bypass configuration information.
	show egress-methods	Replaced by the **show wccp egress** command.

Table 4 CLI Commands Removed in Version 5.0.1 (continued)

Mode	Command	Description
Global configuration	**bypass**	Configures a static bypass list.
	egress-method	Configures WCCP egress method. Replaced by the **egress-method** WCCP configuration command.
	policy-engine	All policy-engine commands are replaced by the **class-map** and **policy-map** commands.
	wccp version 2	Enables or disables WCCP. Replaced by the **enable** WCCP configuration command.

Software Version 5.0.1 Monitoring API Changes

This section includes the following topics:

Software Version 5.0.1 Monitoring API Changes

Table 5 lists the new Monitoring APIs in WAAS version 5.0.1.

Table 5 New Monitoring APIs

Web Service	API Name
AppNavStatsService	retrieveAppNavPassthroughStats
	retrieveAppNavPolicyStats
	retrieveOverallAppNavPolicyStats
	retrieveWNGDistributionStats
IcaStatsService	getBypassedReasons
	getConnStats
	getDroppedReasons
	getEncryptionStats
	getVersionStats
MapiStatsService	retrieveEncryptedAndNonEncryptedOptimizedConnCount
	retrieveEncAndNonEncResponseStats
	retrieveClientSecuredConnCount

Table 5 New Monitoring APIs (continued)

Web Service	API Name
SMBStatsService	getConnOptCount
	getConnOptRate
	getConnOptSavingsByType
	getRequestOptStats
	getTotalConnCount
	retrieveStats
TrafficStatsService	getAllClassMap
	retrieveAverageThroughPutClassStats
	retrieveClassTrafficStats
	retrieveConnectionTrendClassStats
	retrievePeakThroughPutClassStats

Table 6 lists the new Monitoring API objects in WAAS version 5.0.1.

Table 6 New Monitoring API Objects

Web Service	Object Name
AppNavStatsService	AppNavOverallStats
	AppNavPTStats
	AppNavRedStats
	AppNavStats
ICAStatsService	ICABypassedReasons
	ICAConnectionsStats
	ICADroppedReasons
	ICAEncyptStats
	ICAVersionStats
MapiStatsService	MAPIEncAndNonEncOptimizedConnCount
	MAPIEncAndNonEncResponseStats
	MapiClientSecuredConnCount

Table 6 New Monitoring API Objects

Web Service	Object Name
SmbStatsService	SmbConnOptRate
	SmbConnOptSavings
	SmbConnStats
	SmbOptConnCount
	SmbRequestOptStats
	SmbTotalConnCount
TrafficStatsService	AverageThroughputClassStats
	ClassMaps
	ClassifierStats
	ConnectionTrendClassStats
	PeakThroughputClassStats

Table 7 lists the modified Monitoring API objects in WAAS version 5.0.1. These changes are backward compatible with existing code that uses the monitoring API.

Table 7 Modified Monitoring APIs

Web Service	Object Name	Description
Events	MonitoredAO	Added attributes isIcaEnabled and isSmbEnabled to monitor the status of the ICA and SMB accelerators

Using Previous Client Code

If you have upgraded to WAAS version 5.0.1 and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code (prior to 4.3.1) may return unexpected exceptions due to new elements added in the response structures in 4.3.1 and later releases. The observed symptom is an exception related to an unexpected subelement because of the new element (for example, a deviceName element) in the XML response.

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

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

To apply the patch, follow these steps:

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

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

META-INF/
META-INF/MANIFEST.MF
org/
org/apache/
org/apache/axis2/
org/apache/axis2/schema/
```

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

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

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

. . .

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

. . .

<xsl:if test="not(property/enumFacet)">
  else{
```

```
    // A start element we are not expecting indicates an invalid parameter was passed
    // throw new org.apache.axis2.databinding.ADBException("Unexpected subelement " +
reader.getLocalName());
  }
```

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

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

WAAS Documentation Set

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

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Configuring WAAS Express*
- *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*
- *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 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.