# Release Note for Cisco Wide Area Application Services Software Version 5.4.1x

**December 1, 2015**

**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:

- 5.4.1

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

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 5.4.1x:



## Software Version 5.4.1 New and Changed Features

Cisco WAAS Software Version 5.4.1 includes the following new features and changes:

- Akamai Connect is an HTTP/S object cache component added to Cisco WAAS. It is integrated into the existing WAAS software stack and is leveraged via the HTTP Application Optimizer.
  - Helps reduce latency for HTTP/S traffic for business and web applications, and can improve performance for many applications including POS (Point of Sale), HD video, digital signage, and in-store order processing.
  - It provides significant and measurable WAN data offload, and is compatible with existing WAAS functions such as DRE (deduplication), LZ (compression), TFO (Transport Flow Optimization), and SSL acceleration (secure/encrypted) for first and second pass acceleration.
  - Akamai Connect is supported on these platforms:

| Appliance | SM | vWAAS | ISR-WAAS |
|---|---|---|---|
| WAVE-294 | SM-700 | vWAAS-200 | ISR-WAAS-750 (ISR-4451, ISR-4431, ISR-4351, ISR-4331) |
| WAVE-594 | SM-900 | vWAAS-750 | ISR-WAAS-1300 (ISR-4451, ISR-4431) |
| WAVE-694 | SM-710 | vWAAS-1300 | ISR-WAAS-2500 (ISR-4451) |
| | SM-910 | vWAAS-2500 | |
| | | vWAAS-6000 | |

- Enhancements to SMB version 2 Optimization - Cisco WAAS supports SMB v2 application performances and provides improve read-ahead, asynchronous write, and directory listing optimization.
- eMAPI enhancement-- Added support for a single encryption service to support up to 32 matches in order to support hierarchical domain deployments.
- For WAAS version 5.4.1 and later, WAAS supports Windows 2012 R2 domain controllers for obtaining certificates for encrypted protocols such as eMAPI.
- ISR-WAAS supported on ISR-4321, 4331, 4351, and 4431.
- WAAS Central Manager Enhancements - includes Central Manager configuration support for 64 Nodes for AppNav XE devices, customer images on Central Manager reports, availability of single-sided statistics from Central Manager, providing vertical scrollbar view for the Location Tree page and porting of pages (AAA Accounting, Command Authorization, Secure Store, TCP/IP and IP ACL) to the new UI framework.

- CLI commands—For CLI command changes, see the "Software Version 5.4.1 Command Changes" section on page 25.

# Software Version 5.4.1 Filenames

This section describes the Cisco WAAS Software Version 5.4.1 software image files for use on Cisco WAAS appliances and modules and contains the following topics:



## Standard Image Files

Cisco WAAS Software Version 5.4.1 includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- waas-universal-5.4.1.*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-5.4.1.*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-5.4.1.*x*-k9.zip—SM-SRE install .zip file that includes all the files necessary to install Cisco WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-5.4.1.*x*-k9.iso—Cisco WAAS software recovery CD image.
- waas-x86_64-5.4.1.*x*-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- waas-5.4.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.4.1.*x*-k9.bin—Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following the instructions provided by Cisco TAC.
- waas-alarm-error-books-5.4.1.*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 Image Files

Cisco WAAS Software Version 5.4.1 includes No Payload Encryption (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-5.4.1.*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-5.4.1.*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-5.4.1.*x*-npe-k9.zip—SM-SRE install .zip file that includes all the NPE files necessary to install Cisco WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-5.4.1.*x*-npe-k9.iso—Cisco WAAS NPE software recovery CD image.
- waas-x86_64-5.4.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- waas-5.4.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.4.1.*x*-npe-k9.bin—NPE Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following the instructions provided by Cisco TAC.
- waas-alarm-error-books-5.4.1.*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.)

# Cisco WAAS Appliance System Firmware Update

On Cisco Wide Area Application Engine (WAE) and Cisco Wide Area Application Virtualization Engine (WAVE) appliances, we recommend that you update the following three types of system firmware to the latest version to best support new Cisco WAAS features:

- BIOS on the WAVE-294/594/694/7541/7571/8541 models—For details, see the "BIOS Update" section on page 4. 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 5. The latest Baseboard Management Controller (BMC) firmware is required for Intelligent Platform Management Interface (IPMI) over LAN feature.
- RAID controller firmware on the WAVE-7541/7571/8541—For details, see the "RAID Controller Firmware Update" section on page 6. The latest Redundant Array of Independent Disks (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 may also need a BIOS update, though they do not support AppNav.

WAVE-594/694/7541/7571/8541 appliances shipped from the factory with Cisco WAAS Version 5.0.1 or later have the correct BIOS installed. WAVE-294 appliances shipped from the factory with Cisco WAAS Version 5.1.1 or later have the correct BIOS installed.

If you are updating a device that was shipped with an earlier version of Cisco WAAS software, you should update the BIOS, unless it was updated previously. WAVE-594/694 models require BIOS version 18A, WAVE-7541/7571/8541 models require BIOS version 11A, and WAVE-294 models require BIOS version 18A.

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 BIOS firmware update is needed, you can download it from cisco.com at the Cisco Wide Area Application Service (WAAS) Firmware download page (registered customers only). The firmware binary image for WAVE-294/594/694/7541/7571/8541 appliances is named waas-bios-installer-20a-19a-13a-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-20a-19a-13a-k9.bin**

Use the appropriate BIOS installer file for your appliance model.

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—49a
- WAVE-7541/7571/8541—27a

Cisco WAAS appliances shipped from the factory with Cisco 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 Cisco 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 (49a here):

```
wave# show bmc info
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 0.49                    <<<<< version 49
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 Cisco Wide Area Application Service (WAAS) Firmware download page (registered customers only). For example, if the firmware binary image is named waas-bmc-installer-49a-49a-27a-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-49a-49a-27a-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-5 controller firmware for your hardware platform, which can be found on cisco.com at the Cisco 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.

# Upgrading and Interoperability

This section contains the following topics:



## Interoperability and Support

Table 1 lists the hardware, client, and web browser support for Cisco WAAS Software Version 5.4.1.

***Table 1 WAAS 5.4.1 hardware, client and web browser support***

| | |
|---|---|
| Hardware support | The Cisco WAAS software operates on these hardware platforms: WAVE-294, WAVE-594, WAVE-694, WAVE-7541, WAVE-7571, or WAVE-8541 appliance, or an 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 Cisco WAAS Express are supported on the branch side (Cisco WAAS Version 4.2.1 or later is required on the data center side). vWAAS is supported in a Kernel Virtual Machine (KVM) on the Cisco 4451-X Integrated Services Router and on a UCS E-Series module installed in a Cisco ISR G2 or Cisco 4451-X Integrated Services Router, and on other supported VMware virtual machines (for details, see the *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*). You must deploy the Cisco WAAS Central Manager on a dedicated device. |
| Web browser support | The Cisco 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. |

From WAAS version 5.4.1, you are no longer prompted to install the Google Frame plug-in when you access the Central Manager GUI using Internet Explorer. However, if Google Frame plug-in has already been installed earlier, IE will continue using it.

**Note** Akamai Connect is available only on platforms that support 6000 connections or less.

**Note** Akamai Connect and Virtual Blade cannot be run at the same time.

**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). Additionally, we recommend that you clear the browser cache and restart the browser if CIFS device level charts are not visible.

# Cisco WAAS Version Interoperability

Consider the following guidelines when operating a Cisco WAAS network that mixes Software Version 5.4.1 devices with devices running earlier software versions:

- Cisco WAAS Version 5.4.1 is not supported running in a mixed version Cisco WAAS network where any Cisco WAAS device is running a software version earlier than 4.2.1. If you have any Cisco 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 5.4.1. 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 5.4.1 on the Central Manager. Directly upgrading a device from Version 4.0, 4.1, or 4.2 to 5.4.1 is not supported.
- In a mixed version Cisco WAAS network, the Central Manager must be running the highest version of the Cisco WAAS software.

# AppNav Interoperability

Consider the following guidelines when deploying the Cisco AppNav solution:

**AppNav Guidelines:**

- If you are connecting an AppNav Controller (ANC) to a Catalyst 6500 series switch and you have configured the ANC to use the Web Cache Communication Protocol (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 Cisco WAAS nodes in an AppNav deployment must be running Cisco WAAS version 5.0 or later.
- Cisco WAAS Express devices cannot operate as Cisco WAAS nodes in an AppNav deployment.

**AppNav-XE Guidelines:**

- A software version of AppNav, called AppNav-XE, is available on Cisco routers that run Cisco IOS XE Release 3.8 and later but it is not interoperable with Cisco AppNav Controller Interface Modules in the same AppNav Controller group. AppNav-XE can redirect traffic to Cisco WAAS devices for optimization.
- The WAAS Central Manager will not manage AppNav-XE Policy's backup WNG feature that is introduced on Cisco IOS-XE Release 3.13.
- Although an IOS router can have a dot (“.”) in the hostname, this special character is not allowed in a WAAS device hostname. If you try to import an AppNav-XE device that has a dot in the hostname, the import will fail and the following error message is displayed: `Registration failed for the device` *`devicename`* `ConstraintException; Invalid AppNav-XE name: X.X since name includes invalid character '.'.`

# Cisco WAAS Express Interoperability

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

- When using a Cisco WAAS device running version 5.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.2(2)T or earlier, connections originating from the Cisco WAAS device and sent to the Cisco WAAS Express peer are passed through instead of being optimized. We recommend upgrading to Cisco WAAS Express in Cisco IOS Release 15.2(3)T or later to take advantage of the latest enhancements

**Note** As listed in "Software Version 5.1.1 Open Caveats," CSCug16298, "WAAS-X to WAAS 5.1.1 connections will be reset when using HTTP acceleration." We recommend that you do not use HTTP Application Optimizer (AO) between Cisco WAAS and Cisco WAAS Express unless you are running Cisco IOS Release 15.3(1)T or later.

Table 2 lists the support matrix for WAAS Central Manager and IOS-XE release.

***Table 2 WAAS Central Manager and IOS-XE compatibility matrix***

| WAAS Release | IOS XE Release |
|---|---|
| 5.2.x | 3.9 |
| 5.3.x | 3.9, 3.10, 3.11, 3.12 |
| 5.4.x | 3.9, 3.10, 3.11, 3.12, 3.13 |

# WCCP Interoperability

Central Managers running Version 5.4.1x 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.

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 Cisco WAAS software upgrade on all WAEs using the Cisco WAAS Central Manager GUI.

**Step 3** Verify that all WAEs have been upgraded in the Devices pane of the 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** 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
```

# NTLM Interoperability

Cisco WAAS Version 5.1 and later do not support Windows domain login authentication using the NTLM protocol. Therefore, upgrading from a Cisco WAAS Version earlier than 5.1 with the device configured with Windows domain login authentication using the NTLM protocol is blocked. You must change the Windows domain authentication configuration to use the Kerberos protocol before proceeding with the upgrade.

Follow these steps to change from NTLM to Kerberos Windows domain login authentication:

**Step 1** Unconfigure Windows domain login authentication. You can do this from the Central manager in the **Configure** > **Security** > **AAA** > **Authentication Methods** window.

**Step 2** Change the Windows domain configuration setting to use the Kerberos protocol. You can do this from Central manager in the **Configure** > **Security** > **Windows Domain** > **Domain Settings** window. For more information, see the section "Configuring Windows Domain Server Authentication Settings" in the "Configuring Administrative Login Authentication, Authorization, and Accounting" chapter of the *Cisco Wide Area Application Services Configuration Guide*.

**Step 3** Perform the Windows domain join again from the Central manager in the **Configure** > **Security** > **Windows Domain** > **Domain Settings** window.

**Step 4** Configure Windows domain login authentication from the Central manager in the **Configure** > **Security** > **AAA** > **Authentication** Methods window.

**Step 5** Upgrade your device.

**Note** If you are upgrading the Central Manager itself from the GUI and the Windows domain login authentication on the Central Manager is configured to use the NTLM protocol, the upgrade fails with the following error logged in the device log:
Error code107: The software update failed due to unknown reason. Please contact Cisco TAC.

To view the device log for the Central Manager, choose the Central Manager device and then choose **Admin** > **Logs** > **Device Logs**. If you see this error, follow the steps above to change the Central Manager device Windows domain login authentication from NTLM to Kerberos.

If you upgrade the Central Manager itself from the CLI and the upgrade fails due to NTLM being configured, you will get an appropriate error message. Once the Central Manager is upgraded to Version 5.1, it can detect and display the reason for any upgrade failures for other devices.

**Note** Cisco WAAS Version 5.1 and later do not support the Kerberos protocol running with a nonstandard port (other than port 88). Upgrading from a Cisco WAAS Version earlier than 5.1 with the device configured with the Kerberos protocol on a nonstandard port is blocked. You must change the Kerberos server on

your network to listen on port 88 and change the Kerberos configuration on the device to use port 88. You can do this from the Central manager in the **Configure > Security > Windows Domain > Domain Settings** window.

If you are trying to upgrade your device from the CLI and the upgrade fails due to NTLM configuration, then the kerberos_validation.sh script is installed on your device. This script can be used to verify that your network supports the Kerberos protocol before changing from NTLM to Kerberos. This script is not available if you are using the Central Manager to upgrade the device.

To run the script, follow these steps:

**Step 1** (Optional) Run the Kerberos validation script command with the **-help** option to display the usage:

```
CM# script execute kerberos validation.sh -help

Help:
This script does basic validation of Kerberos operation, when device is using NTLM
protocol for windows-domain login authentication.
It can be used as a pre-validation before migrating from NTLM to Kerberos authentication
method.

It does following tests:
1. Active Directory reachability test
2. LDAP server and KDC server availability test
3. KDC service functionality test
   For this test to succeed device must have to join the domain before this test, if not
have joined already.
4. Test for time offset between AD and Device (should be < 300s)

Script Usage:
kerberos_validation.sh [windows-domain name]
For example if Device has joined cisco.com then you need to enter: kerberos_validation.sh
cisco.com
```

**Step 2** Run the Kerberos validation script to verify that your network supports the Kerberos protocol before migrating from NTLM to Kerberos:

```
CM# script execute kerberos validation.sh windows_domain_name

WARNING: For windows authentication operation in 5.1.1, Device will use service on
following ports.
         Please make sure they are not blocked for outbound traffic.
================================================================================
53 UDP/TCP, 88 UDP/TCP, 123 UDP, 135 TCP, 137 UDP, 139 TCP, 389 UDP/TCP, 445 TCP,
464 UDP/TCP, 3268 TCP

Performing following tests on this device.
Test 1: Active Directory reachability test
Test 2: LDAP server and KDC server availability test
Test 3: KDC service functionality test
        For this test to succeed device must have to join the domain before this test, if
not have joined already.
Test 4: Test for time offset between AD and Device (should be < 300s)

Tests are in progress. It may take some time, please wait...

Test 1: Active Directory reachability test : PASSED
Test 2: LDAP server and KDC server availability test : PASSED
Test 3: KDC service functionality test : PASSED
Test 4: Test for time offset between AD and Device (should be < 300s) : PASSED

Validation completed successfully!
```

**Step 3** Change the device Windows domain login authentication from NTLM to Kerberos and upgrade your device, as described in the first procedure in this section.

## Microsoft Windows XP Support

Microsoft ended support for Microsoft Windows XP on April 8, 2014. Microsoft has advised customers to upgrade to a newer Microsoft Windows operating system prior to that date.

Cisco strongly encourages upgrading to the latest Microsoft Windows operating systems. As of October 8, 2014 (six months after Microsoft's end-of-support date), Cisco no longer has support from Microsoft on any Windows XP issues and there is no further testing between Windows XP and WAAS. Any issues specific to Microsoft Windows XP cannot be supported by software updates, and has limited Cisco support after this date.

# Upgrading from a Prerelease Version to Version 5.4.1x

To upgrade from Cisco WAAS prerelease software to Version 5.4.1x, 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 5.4.1x

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 5.4.1x, observe the following guidelines and requirements:

- Upgrading to Version 5.4.1 is supported only from Versions 4.3.x, 4.4.x, 4.5.x, 5.0.x, 5.1.x, 5.2.x and 5.3.x. If you want to upgrade a Cisco WAAS device running an earlier version, first upgrade to one of these supported versions and then upgrade to the current 5.4.1 version.
- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version.
- If you operate a network with devices that have different software versions, the Central Manager must be the highest version and no Cisco WAAS device should be running a version earlier than Version 4.2.1.

- Upgrade the Central Manager devices first, and then upgrade the WAE devices. If you have a standby Central Manager, upgrade it first, before upgrading the primary Central Manager. After upgrading, restart any active browser connections to the Central Manager.
- After upgrading a Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.
- Before upgrading a Cisco WAAS Central Manager, 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 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 5.4.1, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords and CIFS file server passwords. If you do not reenter the passwords, after upgrading to Version 5.4.1, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you use the setup utility for basic configuration after upgrading to 5.4.1, 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.
- In Cisco 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.
- Cisco WAAS Version 5.x no longer supports device group configuration of the following features: static bypass lists, vPath interception, and WCCP. When you are upgrading to Version 5.x 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.
- When upgrading from a Cisco 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 Cisco 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 Cisco WAAS Version earlier than 5.0, classifiers and policies are migrated to new Version 5.x class maps and policy rules. The same functionality is maintained, though the class map and policy framework are different.
- When upgrading a Central Manager from a Cisco WAAS Version earlier than 5.0, the Cisco Wide Area File Services (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 Cisco WAAS device that is still using the WAFS application in a policy rule after an upgrade to Version 5.x 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.
- The ICA application accelerator in Cisco WAAS Version 5.1.1 and later is incompatible with previous releases. During optimization, if the WAE on one side is running a version earlier than 5.1.1 and the WAE on the other side is running Version 5.1.1 or later, all flows being handled by the ICA application accelerator are optimized with transport flow optimization (TFO) only. Both peer WAEs that are participating in the optimization process must be running Cisco WAAS Version 5.1.1 or later to benefit from ICA acceleration features.
- When upgrading to Cisco WAAS Version 5.1 or later, any previous ICA class maps (Citrix-ICA and Citrix-CGP) are combined into a single class map named citrix that is monitored. In addition to matching traffic on ports 1494 and 2598, it includes a new condition that matches a dynamic port associated with the **citrix** protocol to support MSI streams. The enhanced ICA features (WAN secure, MSI support, and DSCP for QoS) are disabled by default.

  The ICA charts in Cisco 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 Cisco WAAS device, the charts appear empty due to the different data that the device is collecting. The ICA data for Version 4.5 Cisco WAAS devices are available in the system level TCP Summary Report by selecting the Remote-Desktop application.
- Cisco WAAS Version 5.1 and later do not support NTLM Windows domain authentication or use of a nonstandard port (other than port 88) for Kerberos authentication. Upgrading from a Cisco WAAS Version earlier than 5.1 is blocked if either of these configurations are detected. You must change these configurations and ensure that your domain controller is configured for Kerberos authentication before proceeding with the upgrade. A script is provided to verify that your network supports Kerberos protocol before migrating from NTLM. For more information, see the "NTLM Interoperability" section on page 10. If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.
- Cisco WAAS Version 5.2 and later restrict the characters used in usernames to letters, numbers, period, hyphen, underscore, and @ sign, and a username must start with a letter or number. Any username not meeting these guidelines is prevented from logging in. Prior to upgrading the Central Manager to Version 5.2 or later, we recommend that you change any such usernames to valid usernames to allow login. For local users, you can do this through the Central Manager **Admin > AAA > Users** page. For remotely authenticated users, you must change the usernames on the remote authentication server.

**Note** Prior to upgrading the Central Manager to Version 5.2 or later, we strongly encourage you to change any usernames that use restricted characters; however if you must maintain existing usernames unchanged, please contact Cisco TAC.

- When you upgrade from Cisco 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.
- Cisco WAAS Version 5.3 and later restricts the use of characters in the name and description field to alphanumeric characters, periods (.), hyphens (-), underscores (), and blank spaces when you create custom reports. When you upgrade from Cisco WAAS Version 4.x and you have custom reports that have special characters in the name or description field, Cisco WAAS automatically removes the special characters from the report name and description, and logs the modification in the central manager system (CMS) logs.

# Migrating a Central Manager from an Unsupported Platform

If you have a Cisco WAAS Central Manager that is running on a hardware platform that is unsupported in Version 5.1 and later (such as a WAE-511/512/611/612/7326 or NME-WAE module), you are not allowed to upgrade the device to Version 5.1 or later. 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 Cisco 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 backup/cms-db-06-28-2012-15-08_5.0.1.0.15.dump
Backup file backup/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# cd /local1/backup
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 Cisco WAAS Version 5.1. 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 backup/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 Cisco 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 Cisco WAAS Version 5.1.x or later. 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 Cisco WAAS devices are shown in an online state in the Devices window.

**Step 13** (Optional) Register a new standby Central Manager that is running Cisco WAAS Version 5.1.x or later.

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

Wait for the device to reload, change the Central Manager role to standby, and register the standby Central Manager to the primary Central Manager.

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

# Migrating a physical appliance being used as a Central Manager to a vCM

Follow these steps to migrate a primary Central Manager to a vCM:

**Step 1** Introduce vCM as the Standby Central Manager by registering it to the Primary Central Manager.

**Step 2** Configure both device and device-group settings through Primary CM and ensure that devices are getting updates. Wait for two to three data feed poll rate so that the Standby CM gets configuration sync from the Primary CM.

**Step 3** Ensure that the Primary CM and Standby CM updates are working.

**Step 4** Switch over CM roles so that vCM works as Primary CM. For additional details please refer to "*Converting a Standby Central Manager to a Primary Central Manager*" section of the WAAS Configuration Guide.

# 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 Cisco 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 5.4.1x to a Previous Version

Note the following guidelines and considerations for downgrading:

- Downgrade is supported only to Versions 4.3.x, 4.4.x, 4.5.x, 5.0.x, 5.1.x, and 5.2.x. Downgrade is not supported to Versions 4.2.x through 4.0.x.
- After downgrading a Cisco WAAS Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.
- On the Cisco 4451-X Integrated Services Router running ISR-WAAS, downgrading to a version earlier than 5.2.1 is not supported.
- On the UCS E-Series Server Module installed in a Cisco ISR G2 Router and running vWAAS, downgrading to a version earlier than 5.1.1 is not supported. On the UCS E-Series Server Module installed in the Cisco 4451-X Integrated Services Router and running vWAAS, downgrading to a version earlier than 5.2.1 is not supported. On other vWAAS devices you cannot downgrade to a version earlier than 4.3.1.
- If the Central Manager is downgraded to a version earlier than 5.2.1, it can no longer manage AppNav-XE clusters and devices and all related configuration records are removed.
- If the Central Manager is downgraded to a version up to 5.2.1 and if the AppNav-XE cluster has more than 32 WAAS nodes, it is recommended to reduce the number of WAAS nodes to a maximum of 32 prior to downgrade.
- On WAVE-294/594//8541 models with solid state drives (SSDs) you cannot downgrade to a version earlier than 5.2.1.
- On WAVE-294/594/694/7541/7571/8541 models you cannot downgrade to a version earlier than 4.4.1.
- When downgrading Cisco 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 Cisco WAAS versions earlier than 5.0.1 and is nonfunctional after a downgrade.
- 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.
- 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 Cisco WAAS to a version earlier than 4.4.5.

To downgrade the Cisco 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 backup/cms-db-06-28-2012-15-08_5.0.1.0.15.dump
Backup file backup/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# cd /local1/backup
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 Cisco 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 for the respective Cisco WAE and WAVE appliance.

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 Cisco WAAS Software Version 5.4.1x and contains the following topics:



## Central Manager Report Scheduling

In the Cisco 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.

## Cisco WAAS Express Policy Changes

Making policy changes to large numbers of Cisco WAAS Express devices from the Central Manager may take longer than making policy changes to Cisco 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 Cisco 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 Cisco 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 Cisco 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 login page. To avoid this prompt, remove the installed personal certificates or use a different browser.

## Default Settings with Mixed Versions

If a Central Manager is managing Cisco WAAS devices that have different versions, it is possible that a feature could have different default settings in those different versions. If you use the Central Manager to apply the default setting for a feature to mixed devices in a device group, the default for the Central Manager version is applied to all devices in the group.

# Software Version 5.4.1x Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, command changes, and monitoring API changes in Software Version 5.4.1x and contains the following topics:

# Software Version 5.4.1a Resolved Caveats

The following caveats were resolved in software version 5.4.1a.

| Caveat ID Number | Headline |
|---|---|
| CSCul35517 | ICAAO resetting connections - BASIC Encryption Permanent |
| CSCuq35618 | SMBAO serves invalid data for file access |
| CSCuq46631 | Multiple Vulnerabilities in OpenSSL - August 2014 |
| CSCuq62010 | 'decode_arlindex' binary gets corrupted during build packaging |
| CSCuq14788 | HTTP Active connection count is more than TFO limit |
| CSCue47674 | WAAS partial denial of service vunlerability |
| CSCum85942 | Connections impacted after Appnav controller reloaded |
| CSCuo79094 | cwoAoStatsStartUpTime mib value inconsistent |
| CSCuo90701 | WAE sends attribute in an incorrect format for command authorization. |
| CSCuq81128 | Consolidation getting failed in specific scenario |

# Software Version 5.4.1a Open Caveats

The following caveats are open caveats for Software Version 5.4.1a. Note that there might be additional open caveats from the previous release that are applicable to this release, unless they are specifically listed as resolved. For details, see the “Software Version 5.4.1 Open Caveats” section.

# Software Version 5.4.1 Resolved Caveats

The following caveats were resolved in Software Version 5.4.1.

| Caveat ID Number | Headline |
|---|---|
| CSCty62412 | “Processor P0 CATERR” entry is logged in bmc event log |
| CSCuo81272 | Duplicate Key message in syslog |
| CSCua02585 | BMC timer not getting reset properly |
| CSCui12945 | Unable to update "IP ACL Condition" after changing order |
| CSCui12966 | "Edit Condition" may result in editing undesired condition |
| CSCuc05659 | core.more files created in specific cases |
| CSCuh47000 | Update the Intel Ethernet driver (igb) to 3.2.9 or later |
| CSCuj18149 | kernel msg "response: Error 2 cmd 3" is seen in syslog |
| CSCuo24261 | cpmCPUTotal1minRev and 5minRev OID not available on WAAS Central Manager |

| Caveat ID Number | Headline |
|---|---|
| CSCun96883 | Secondary CM unable to register to Primary CM |
| CSCun62778 | WAAS SSL-AO break traffic, when server request Client Auth Certificate. |
| CSCun50281 | Waas express router enters override status after reload |
| CSCun16434 | To raise an alarm when SMB Matadata Cache reaches Max limit |
| CSCum99983 | SR Core seen while clear the blacklist identity in specific scenario |
| CSCum83854 | CIFS acceleration randomly reporting delayed keepalives |
| CSCum67339 | CM GUI misleading with LCM disabled |
| CSCum27787 | CM dashboard page and all monitoring pages throws error |
| CSCum15748 | configuring snmp view and responding to the query results in snmp core |
| CSCul73734 | WAAS CM login will fail for users when TACACS send a message |
| CSCul66264 | All Standard Time Zone values result in UTC offset of zero |
| CSCul52341 | Encrypted MAPI fails when users have non-ASCII names |
| CSCul50491 | WAAS - CMS service reporting OOM messages in log files |
| CSCul35633 | WAAS encryption-service identity failing to join on error |
| CSCuj83145 | SSL Global Setting page and System Log page overridden at device level |
| CSCuj38649 | CM GUI does not allow disable "Enable Export" under Transaction logging |
| CSCui64777 | WAAS CM can't communicate with Accelerators |
| CSCui57813 | In rare case sysmon deamon may become stuck and processes don't release |
| CSCui44659 | Cannot login/create user on device due to group file lock |
| CSCuh44297 | WAAS Kernel Crash due to 'struct sk_buff' memory handlers |
| CSCue42754 | Documentation of disk status LED is not accurate |
| CSCuc94420 | Optimized connections exceeding Device Limit |

# Software Version 5.4.1 Open Caveats

The following open caveats apply to Software Version 5.4.1.

| Caveat ID Number | Headline |
|---|---|
| CSCum17724 | Office365: Lync application login failure when WAAS optimize SSL traffic |
| CSCum92402 | NTLM key retrieval fails when child user login with parent upn suffix |
| CSCum90791 | Adding Identity along with more than 2 match from CM fails with error |
| CSCum85942 | Connections impacted on ANC reload |
| CSCud31131 | vPATH: Performance drop is seen when running HTTP traffic |
| CSCup80526 | Stuck connections seen when running HTTP traffic with AK connect enabled |
| CSCuq14788 | HTTP Active connection count is more than TFO limit |
| CSCuq29566 | Sharepoint pre-fetch benefit is not seen when Akamai Connect is enabled |
| CSCul52956 | SMB connections stay indefinitely on WAEs |

| Caveat ID Number | Headline |
|---|---|
| CSCul72538 | cifs cache corruption under rare scenario |
| CSCuo78582 | SMBAO restarts rarely while handling FF or FN in a specific scenario |
| CSCup72141 | SMB AO restarts in a rare situation |
| CSCuo64013 | WAAS - AppNav module missed keepalives |
| CSCuo90677 | Observed nprm service died while change device-mode scenario |
| CSCup47679 | Packet loss and FCS errors reported by IOM interface |
| CSCuq11794 | Performance Degradation seen in vWaas 6000 Encode test |
| CSCuq19619 | WAAS Unexpected Reboot |
| CSCum12858 | Kernel crash in BNX2 driver |
| CSCuo07060 | WAAS Crash with Core - Oracle sleepycat DB |
| CSCup75956 | In specific scenario, Java process restart seen |
| CSCum41681 | WAAS: ica_ao64 core generated on device |
| CSCum46164 | Well known certs expiring |
| CSCtn31868 | nscd service dead alarm raised and cleared in WAE periodically |
| CSCty14254 | Standby Interface failover to primary not sendng gratuitous ARP |
| CSCua35619 | JSF Exceptions seen while submitting config changes from Central Manager |
| CSCua38244 | Internet Explorer browser may exit when user clicks on telnet:// link |
| CSCud28450 | Standby primary-int is  in inactive state during Upgrade/downgrade |
| CSCud94009 | show inventory shows the transceiver still present even after removing. |
| CSCue73675 | WAAS: Multiple Features not working with Management Interface |
| CSCuf35560 | Waas resets conn when inline wan gets packet leaked from remote lan |
| CSCuh01175 | Application freezes with ICAoSSL during network flap on XenApp server |
| CSCuh41218 | Session reliability does not happen for Multi stream ICAoSSL connection |
| CSCuh69340 | Rarely, SMB-AO in restarts with SMBv1 traffic |
| CSCum06336 | Add support for handling unicode characters in username/domainname |
| CSCuq99916 | DNS server issues will fail Akamai Connect to start properly |
| CSCur01979 | OTT range requests cause OTT videos to not be cached |
| CSCur01984 | Ad blocking software stops OTT videos from loading |
| CSCur01991 | ACC, OTT can override explicit bypass rules |

# Software Version 5.4.1 Command Changes

This section lists the new and modified commands in Cisco WAAS Software Version 5.4.1.

Table 3 lists the commands and options that have been added in Cisco WAAS Software Version 5.4.1.

***Table 3 CLI Commands Added in Version 5.4.1***

| Mode | Command | Description |
|---|---|---|
| EXEC | **clear cache http-object-cache invalidate** | Clears the object cache. |
| | **debug accelerator http object-cache** | Enables object-cache debugging. |
| | **show accelerator http object-cache** | Displays HTTP object cache configuration and status information for a WAAS device. |
| | **show statistics accelerator http object-cache** | Displays object cache statistics for a WAAS device. |
| | **clear statistics accelerator http object-cache** | Clears object cache statistics for a WAAS device. |
| | **show statistics accelerator http preposition** | Displays preposition task information for a WAAS device. |
| **Global configuration** | **accelerator http object-cache enable** | Turns on the cache engine for the WAE. |
| | **accelerator http object-cache transparent enable** | Enables transparent caching mode on the cache engine. |
| | **accelerator http object-cache transparent basic** | Enables transparent basic caching mode on the cache engine. |
| | **accelerator http object-cache transparent standard** | Enables transparent standard caching mode on the cache engine. |
| | **accelerator http object-cache transparent advanced** | Enables transparent advanced caching mode on the cache engine. |
| | **accelerator http object-cache transparent bypass** | Turns off caching for a configured site. |
| | **accelerator http object-cache ott enable** | Turns on OTT caching mode for the cache engine to cache content from YouTube. |
| | **accelerator http object-cache connected enable** | Enables the cache engine to retrieve content from Akamai's CDNs (Content Data Networks). |
| | **accelerator http object-cache cws-check enable** | Enables the Cisco Cloud Web Security feature. |
| **Config Prep** | **accelerator http preposition dre enable** | Enables DRE for preposition connections. |
| | **accelerator http preposition task task-name** | Configures a preposition task for one or more sites. |

Table 4 lists existing commands that have been modified in Cisco WAAS Version 5.4.1.

***Table 4 CLI Commands Modified in Version 5.4.1***

| Mode | Command | Description |
|---|---|---|
| EXEC | **show statistics accelerator ica [detail]** | Added field descriptions for show statistics accelerator ica [detail] |
| | **debug cms {router-config \| stats}** | Added keyword router-config to enable debug only router configuration from CM<br>Added keyword stats to enable debug only statistics |
| Global configuration | **accelerator smb** | Added the keywords smb2.x-read-caching enable and smb2.x-write-optimization enable options to enable smb2 read caching and smb2.x write optimization. |

## Using Previous Client Code

If you have upgraded to Cisco WAAS Version 5.4.1 and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code (prior to 4.3.1) may return unexpected exceptions due to new elements added in the response structures in 4.3.1 and later releases. The observed symptom is an exception related to an unexpected subelement because of the new element (for example, a deviceName element) in the XML response.

To work around this problem, we recommend that you patch the WSDL2Java tool library to silently consume exceptions if new elements are found in XML responses 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;&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** Re-create 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.

# Cisco 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*
- *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*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *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 "Cisco WAAS Documentation Set" section.