Release Note for Cisco Wide Area Application Services Software Version 5.1.1x

June 12, 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:

- 5.1.1i
- 5.1.1h
- 5.1.1g
- 5.1.1f
- 5.1.1e
- 5.1.1d
- 5.1.1.c
- 5.1.1b
- 5.1.1a
- 5.1.1

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:

New and Changed Features

The following sections describe the new and changed features in software Version 5.1.1x:

Software Version 5.1.1 New and Changed Features

WAAS software Version 5.1.1 includes the following new features and changes:

- ICA Application Accelerator—Enhanced to optimize multi-stream ICA (MSI) traffic, to provide QoS support for MSI and non-MSI ICA streams, to provide better compression, and to provide better WAN secure performance. The ICA application accelerator requires that both peer WAAS devices are running WAAS version 5.1.
- HTTP Accelerator—Enhanced to optimize Sharepoint traffic.
- vWAAS—vWAAS now operates under ESXi 5.0 on the UCS E-Series Server Module installed in an ISR G2 router.
- Central Manager—Enhanced by updating more pages to the new user interface that was introduced in version 5.0.1.

- AAA—Upgraded to remove Samba, increase stability, and drop support for NTLM authentication. Any devices that are using NTLM Windows domain authentication must be changed to Kerberos authentication on standard port 88 before upgrading to version 5.1.1. For more information, see NTLM Interoperability. Additionally, the Windows Authentication tab was removed from the device manager GUI.
- NME-WAE-502 modules—This module is no longer supported and WAAS version 5.1 and later does not operate on any NME-WAE modules. Upgrading to WAAS version 5.1 on this module (or on a device group that contains any of these modules) is not allowed.
- CLI commands—For CLI command changes, see the Software Version 5.1.1 Command Changes.

Software Version 5.1.1 Filenames

This section describes the WAAS software Version 5.1.1 software image files for use on WAAS appliances and modules and contains the following topics:

Standard Image Files

WAAS software Version 5.1.1 includes the following standard primary software image files for use on WAAS appliances and modules:

- waas-universal-5.1.1.*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-5.1.1.*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-5.1.1.*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-5.1.1.*x*-k9.iso—WAAS software recovery CD image.
- waas-x86_64-5.1.1.*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-5.1.1.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.1.1.*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-5.1.1.*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 5.1.1 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-5.1.1.*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-5.1.1.*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-5.1.1.*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-5.1.1.*x*-npe-k9.iso—WAAS NPE software recovery CD image.
- waas-x86_64-5.1.1.*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-5.1.1.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-kdump-5.1.1.*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-5.1.1.*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-294/594/694/7541/7571/8541 models—For details, see BIOS Update. The latest BIOS is required for AppNav operation.
- BMC firmware on the WAVE-294/594/694/7541/7571/8541 models—For details, see BMC Firmware Update. 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 RAID Controller Firmware Update. 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 may also need a BIOS update, though they do not support AppNav.

WAVE-594/694/7541/7571/8541 appliances shipped from the factory with WAAS version 5.0.1 or later have the correct BIOS installed. WAVE-294 appliances shipped from the factory with 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 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 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 for WAVE-294/594/694/7541/7571/8541 appliances is named waas-bios-installer-18a-18a-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**

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—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 5.1.1.

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 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 4.3.1 or later is required on the data center side). vWAAS is supported on a UCS E-Series module installed in an ISR G2 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 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 5.1.1 devices with devices running earlier software versions:

- WAAS Version 5.1.1 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 5.1. 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 5.1.1 on the WAAS Central Manager. Directly upgrading a device from version 4.0, 4.1, or 4.2 to 5.1 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.
- A software version of AppNav is available on routers that run IOS-XE Release 3.8 but it is not interoperable with Cisco AppNav Controller Interface Modules in the same AppNav Controller group. AppNav on IOS-XE can redirect traffic to WAAS devices for optimization.

WAAS Express Interoperability

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

- When using a WAAS device running version 5.x 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.

Note CSCue80300 was resolved in software version 5.1.1e. This allows WAAS Express-enabled routers to inter-operate with WAAS nodes above version 5.03x.

Note CSCug16298 was resolved in Cisco IOS 15.2(4)M and later. We recommend that you do not use HTTP AO between WAAS and WAAS Express without running Cisco IOS 15.2(4)M and later or Cisco IOS 15.3(1)T and later.

Note As listed in “Software Version 5.1.1 Open Caveats,” CSCue80300, WAAS Express-enabled routers cannot inter-operate with WAAS nodes above version 5.0.3x.

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.” It is recommended to not use HTTP AO between WAAS and WAAS Express until DDTS CSCug16298 is resolved in IOS.

WCCP Interoperability

Central Managers running Version 5.1.1x 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 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 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

WAAS version 5.1 does not support Windows domain login authentication using the NTLM protocol. Therefore, upgrading from a 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 WAAS version 5.1 does not support the Kerberos protocol running with a nonstandard port (other than port 88). Upgrading from a 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 won't be 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.

Upgrading from a Prerelease Version to Version 5.1.1x

To upgrade from WAAS prerelease software to Version 5.1.1x, 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 5.1.1x

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 5.1.1x, observe the following guidelines and requirements:

- Upgrading to Version 5.1.1 is supported only from Versions 4.3.x, 4.4.x, 4.5.x, and 5.0.x. If you want to upgrade a WAAS device running an earlier version, first upgrade to one of these supported versions and then upgrade to the current 5.1.1 version.
- Upgrading to Version 5.1.1 is not supported on the following platforms: WAE-511, WAE-512, WAE-611, WAE-612, WAE-7326, NME-WAE-302, NME-WAE-502, and NME-WAE-522. WAAS Version 5.1 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 Migrating a Central Manager from an Unsupported Platform.

- 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 5.1.1, 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 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 5.1.1, 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 5.1.1, 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 5.1.1, 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 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.
- 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 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.x 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.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 WAAS version 5.1.1 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 TFO only. Both peer WAEs that are participating in the optimization process must be running WAAS version 5.1.1 or later to benefit from ICA acceleration features.
- When upgrading to WAAS version 5.1, 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 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.
- WAAS version 5.1 does not support NTLM Windows domain authentication or use of a nonstandard port (other than port 88) for Kerberos authentication. Upgrading from a 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 NTLM Interoperability. If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.
- 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 5.1 (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. 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 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 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 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 5.1.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 5.1.x.

```
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
```

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 5.1.1x 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, and 5.0.x. Downgrade is not supported to versions 4.2.x through 4.0.x.
- On the UCS E-Series Server Module running vWAAS, downgrading to a version earlier than 5.1.1 is not supported. On other vWAAS devices 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.
- 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 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 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 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 5.1.1x 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.

Multiple vWAAS Appliances

If multiple vWAAS appliances are deployed, a conflict of DRE peer ID owners may occur on the core WAE side. This causes any DRE optimized connections to get reset by the core WAE, disrupting traffic.

To reset unique IDs back for the active connections, follow these steps:

Step 1 Run the **vm.init** command on affected vWAAS devices.

Step 2 Reload device.

You can also run the **clear_dre.sh** script to resolve this situation. Please contact your Cisco representative to obtain a copy of this script.

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.

Default Settings with Mixed Versions

If a Central Manager is managing 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 5.1.1i Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software version 5.1.1i and contains the following topics:

Software Version 5.1.1i Resolved Caveats

The following caveats were resolved in software version 5.1.1i.

Caveat ID Number	Description
CSCus69606	Evaluation of glibc GHOST vulnerability - CVE-2015-0235
CSCut29360	False SIA invalid pkt alarm seen in Service Node
CSCut27453	match tcp dest ip 0.0.0.0 255.255.255.255' translated wrongly by CLI
CSCut44516	SSLv3 need to be removed from CM GUI
CSCus31326	Oct 2014 OpenSSL Vulnerabilities (CVE-2014-3513 CVE-2014-3567 CVE-2014-3568)
CSCut46458	MARCH 2015 OpenSSL Vulnerabilities (CVE-2015-0291 CVE-2015-0204 CVE-2015-0290 CVE-2015-0207 CVE-2015-0286 CVE-2015-0208 CVE-2015-0287 CVE-2015-0289 CVE-2015-0292 CVE-2015-0293 CVE-2015-1787 CVE-2015-0285 CVE-2015-0288)
CSCus42766	JANUARY 2015 OpenSSL Vulnerabilities (CVE-2014-3569 CVE-2014-3570 CVE-2014-3571 CVE-2014-3572 CVE-2014-8275 CVE-2015-0204 CVE-2015-0205 CVE-2015-0206)
CSCue89554	OpenSSL Multiple Vulnerabilities CVE-2013-0169
CSCuu43800	Policy page overridden in device level after restoring policies from DG

Software Version 5.1.1i Open Caveats

The following open caveats apply to software version 5.1.1i. The open caveats for software version 5.1.1i are the same as those for software version 5.1.1h, except for those that are resolved in version 5.1.1i. For more details, see the Software Version 5.1.1h Open Caveats. Note that these open caveats also apply to all previous releases of 5.1.1x, including Software Version 5.1.1 Open Caveats.

Caveat ID Number	Description
CSCuo64013	WAAS - AppNav module missed keepalives
CSCua38244	Internet Explorer browser may exit when user clicks on telnet:// link
CSCud28450	Appnav IOM: Standby primary-int is in inactive state
CSCue75447	Pidof core file created on WAAS device

Software Version 5.1.1h Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software version 5.1.1h and contains the following topics:

- Software Version 5.1.1h Resolved Caveats
- Software Version 5.1.1h Open Caveats

Software Version 5.1.1h Resolved Caveats

The following caveats were resolved in software version 5.1.1h.

Caveat ID Number	Description
CSCur02917	WAAS evaluation for CVE-2014-6721 and CVE-2014-7169

Software Version 5.1.1h Open Caveats

The open caveats for software version 5.1.1h are the same as those for software version 5.1.1g, except for those that are resolved in version 5.1.1h. For details, see the Software Version 5.1.1g Open Caveats.

Software Version 5.1.1g Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software version 5.1.1g and contains the following topics:

- Software Version 5.1.1g Resolved Caveats
- Software Version 5.1.1g Open Caveats

Software Version 5.1.1g Resolved Caveats

The following caveats were resolved in software version 5.1.1g.

Caveat ID Number	Description
CSCuf35699	Pause Frames seen in the AppNav card
CSCuh47000	Update the Intel Ethernet driver (igb) to 3.2.9 or later
CSCul77971	SIA invalid packets are detected in service-node alarm
CSCum97997	Alarm not raised for DRE and swap partition sizes
CSCun06499	CMS subsystem continuously logging rollback messages
CSCun70617	Syslog periodically reporting DataServer GenId mismatch WafsGenId
CSCup22648	Multiple Vulnerabilities in OpenSSL - June 2014
CSCuq46631	Multiple Vulnerabilities in OpenSSL - August 2014

Software Version 5.1.1g Open Caveats

The open caveats for software version 5.1.1g are the same as those for software version 5.1.1f, except for those that are resolved in version 5.1.1g. For details, see the Software Version 5.1.1f Open Caveats.

Software Version 5.1.1f Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software version 5.1.1f and contains the following topics:

- Software Version 5.1.1f Resolved Caveats
- Software Version 5.1.1f Open Caveats

Software Version 5.1.1f Resolved Caveats

The following caveats were resolved in software version 5.1.1f.

Caveat ID Number	Description
CSCup80684	Implement np restart in WAAS code for NP controller issues
CSCum77623	WAAS - so_dre created a file on system

Software Version 5.1.1f Open Caveats

The open caveats for software version 5.1.1f are the same as those for software version 5.1.1e, except for those that are resolved in version 5.1.1f. For details, see the Software Version 5.1.1e Open Caveats.

Software Version 5.1.1e Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software Version 5.1.1e and contains the following topics:

Software Version 5.1.1e Resolved Caveats

The following caveats were resolved in software Version 5.1.1e.

Caveat ID Number	Description
CSCud81728	WAE is sending malformed pages to client resulting in unexpected error
CSCud81989	Mapi creates coredump in SM-SRE after upgrading from 5.0.3 to 5.1.1
CSCud95802	so_dre coredumps instead of fallback to LZ only when invalid cache size
CSCue18479	httpmuxd restarted and created core file with SharePoint traffic
CSCue41034	WAVE-594 issue with usb "lsusb, copy usb install and copy sysreport usb"
CSCue57443	so_dre core created when running 50% decode perf test on vWAAS 2500
CSCuf35038	Mapi AO core file and restart under rare scenario durin session shutdown
CSCuf52374	MAPI AO core - retry timer expired
CSCug23442	domain identity fails to create with multiple ip domains configured
CSCug59333	Rarely, standby central manager may miss database updates
CSCug73981	CM unable to send cold-start trap after reload
CSCug83483	httpmuxd process restarted and created core file in "freeStringBufferMan
CSCug97824	DRE error results in Memory allocation failure
CSCuh04512	Encryption-service fails to retrieve key from AD with renamed domain
CSCuh17673	After upgrade to 5.1.1x - conns going PT Peer AOIM Sync in Pr
CSCuh41103	WAAS fails to clear alarm on Central Manager
CSCuh42989	HTTP connection gets reset due to cs_RELAY IoRdWn cmd pending already
CSCuh46866	Observing java "OutofMemoryError" Exceptions in a scenario
CSCuh52199	Machine Acc DI removed on reload when wkgrp is diff than 1st part of dom
CSCui09533	WAAS 5.2.1 EMAPI dropping users even though encryption not configured
CSCui20405	WAAS: BMC software update fails through USB
CSCui25198	Large File Copy failed when using CifsAO
CSCui36175	WAAS: FTP issue with mixed versions
CSCui82284	CM page loading issues in Chrome browser version- 29
CSCuj02926	WAAS MAPI-AO optimized connections lead to stuck email in O2K7 outbox
CSCuj77355	Wrong files/folders are seen with dynamic-share + ABE in cifsao

Caveat ID Number	Description
CSCuj77363	Wrong files/folders are seen with dynamic-share with aliases Domain
CSCuj96948	WAAS will prevent signed SMB traffic, causing access-denied errors
CSCul24050	Memory leak observed on WAAS device in SMBAO process
CSCul41376	Group level statistics periodically show dip in CM GUI

Software Version 5.1.1e Open Caveats

The open caveats for software Version 5.1.1e are the same as those for software Version 5.1.1d, except for those that are resolved in Version 5.1.1e. For details, see the Software Version 5.1.1d Open Caveats.

Software Version 5.1.1d Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software Version 5.1.1c and contains the following topics:

- Software Version 5.1.1d Resolved Caveats
- Software Version 5.1.1d Open Caveats

Software Version 5.1.1d Resolved Caveats

The following caveats were resolved in software Version 5.1.1d.

Caveat ID Number	Description
CSCuf50741	Temporary png files not moved after generating PDF report
CSCuf60155	Apply default in adaptive buffer page is not working as expected
CSCuh20849	ApplNav class maps not accepting certain IP netowrks in CM GUI
CSCuh20864	AppNav Class-Map of type Customer does not accept wildcard mask
CSCuh20882	Pass-through offloading settings propagation to ANCs inconsistent
CSCuh43629	HTTP accelerator loggin error upon processing CONNECT request
CSCuh58350	CIFS-AO Debug messages not rate limited
CSCuh67012	ICA AO generated core file during load traffic with encryption
CSCui15043	Connection from NetApp filer to Domain Controller fails through WAAS
CSCui25002	Win7 client robocopy cannot copy files between directories on server
CSCug47777	Data mismatch seen in AppNav reports when scope is Device

Software Version 5.1.1d Open Caveats

The open caveats for software Version 5.1.1d are the same as those for software Version 5.1.1c, except for those that are resolved in Version 5.1.1d. For details, see the Software Version 5.1.1c Open Caveats.

Software Version 5.1.1c Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software Version 5.1.1c and contains the following topics:

Software Version 5.1.1c Resolved Caveats

The following caveats were resolved in software Version 5.1.1c.

Caveat ID Number	Description
CSCue80300	Connection (TFO+LZ only) reset when peer is WAAS-Express
CSCug24906	DRE Core File on WAAS device for 5.1.1b code
CSCtz95815	Apache HTTPD Server Version Out of Date
CSCuc71539	Backward slash changed to Forward slash by WAAS in CIFS AO
CSCue25543	HTTPAO improperly caches 401 from URL's longer than 255 characters
CSCue71029	WAAS - alarm for file on system
CSCuf20693	HTTPmuxd restarted created core due to memory corruption in alloc lib
CSCuf38893	Outlook 2010 Client connections with missing AuxBuffer are not optimized
CSCuf50145	SMBFD read failed creating SMBAO core dump
CSCuf85678	Connection Failing/RST when ServerGUID doesn't exist
CSCuf95580	In a specific situation, new files cannot be created using default names
CSCug01198	CM Menu items alignment issue in Chrome browser version- 26
CSCug03362	WAAS SMB AO prompts XP user when saving 2002/2003 Excel file
CSCug19409	7571 inline WAN interface up/up on reload with just WAN port connected

Software Version 5.1.1c Open Caveats

The open caveats for software Version 5.1.1c are the same as those for software Version 5.1.1b, except for those that are resolved in Version 5.1.1c. For details, see the Software Version 5.1.1b Open Caveats.

Software Version 5.1.1b Resolved and Open Caveats

Software Version 5.1.1b Resolved Caveats

The following caveats were resolved in software Version 5.1.1b.

Caveat ID Number	Description
CSCuf33319	MAPI AO failure when user and server are in different realms
CSCud44425	WAAS - SMB_AO Core file generated on file system
CSCud48222	ica core dump generated by possible older citrix client
CSCud65388	WAAS - so_dre64 file created on file system
CSCud67495	SMB3 client unable to access SMB2 share if highest dialect set to SMB1
CSCud88090	WAAS Express to WAAS ICA AO auto discovery flow causes traceback on ISR
CSCud89871	Enhance DClocator faicility to do explicit name resolution
CSCud98635	WAAS 5.0.1 - so_dre core file created on file system
CSCue05644	SMB share not accessible : Client-Win8 Server-W2k8 SP1
CSCue10563	Inline interception card interrupts traffic during reload on 594 8541
CSCue11874	WAAS core in SMBAO process
CSCue14467	MAPI Connections dropped followed with multiple core file generation
CSCue34069	Memory leaks in emapi code
CSCue50647	Ica traffic got strucked in edge device during stress
CSCue60091	Some Citrix clients unable to connect through ICA AO after WAAS upgrade
CSCue93445	DceRpc Frag reader overloaded nWantedSize leading to disconnection
CSCue94114	TOP utility needs to be run in secure mode in WAAS

Software Version 5.1.1b Open Caveats

The open caveats for software Version 5.1.1b are the same as those for software Version 5.1.1a, except for those that are resolved in Version 5.1.1b. For details, see the Software Version 5.1.1a Open Caveats.

Software Version 5.1.1a Resolved and Open Caveats

This section contains the resolved caveats and open caveats in software Version 5.1.1a and contains the following topics:

- Software Version 5.1.1a Resolved Caveats
- Software Version 5.1.1a Open Caveats

Software Version 5.1.1a Resolved Caveats

The following caveats were resolved in software Version 5.1.1a.

Caveat ID Number	Description
CSCud77164	CM UI may hang occasionally in deployment with WAAS express devices
CSCud98825	MAPI-AO crashed due to Stub convertor fragment alignment assert
CSCue47325	AppNav controller home page shows error under certain configuration

Software Version 5.1.1a Open Caveats

The open caveats for software Version 5.1.1a are the same as those for software Version 5.1.1, except for those that are resolved in Version 5.1.1a. For details, see the Software Version 5.1.1 Open Caveats.

Software Version 5.1.1 Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, command changes, and monitoring API changes in software Version 5.1.1 and contains the following topics:

- Software Version 5.1.1 Resolved Caveats
- Software Version 5.1.1 Open Caveats
- Software Version 5.1.1 Command Changes

Software Version 5.1.1 Resolved Caveats

The following caveats were resolved in software Version 5.1.1.

Caveat ID Number	Description
CSCtd70016	Under rare circumstances, CIFS AO can not be re-enabled
CSCtz24645	ICA: Sever lag seen while typing text and playing a video for 300 conn
CSCsi65522	CIFS related statistics graphs are not populated.Tracking of MRTG upgrad
CSCtz13223	WAAS CIFS AO will produce a java hprof for scanning tool SMB request
CSCtz78575	HTTP-AO prevents FIN flag reaching the client
CSCub21189	WAAS Express configuration may not be propagated from CM GUI
CSCub26344	Code dump in device manager due to signal handler conflict
CSCuc05753	SRE710 shutdown button not work and output error

Software Version 5.1.1 Open Caveats

The following open caveats apply to software Version 5.1.1. Note that open caveats for software version 511i also apply to software version 511.

Caveat ID Number	Description
CSCud28450	Appnav IOM: Standby primary-int is in inactive state
CSCum77623	WAAS - so_dre created a file on system
CSCtu24846	Mixed AO tests: fb_hashtbl_delete Attempted to delete a filetring tuple
CSCtx55758	packet-capture CLI fails to account for WCCP GRE
CSCtx61799	Both PSU (PSU1 and PSU2) missing alarm on WAVE-7541
CSCty14254	Standby Interface failover to primary not sendng gratuitous ARP
CSCtz20636	Alarm update ignored when CM received it after device is Offline
CSCtz74336	WAN secure AO Callback along with dropped MAPI conenctions
CSCua35619	JSF Exceptions seen while submitting config changes from Central Manager
CSCua38244	Internet Explorer browser may exit when user clicks on telnet:// link
CSCua55674	Changes not to render M&R Charts with insufficient data in few cases
CSCua64691	Launch of NAM UI fails from CM gui on IE8 with Google chrome plug-in
CSCub76628	KDUMP file created on vWAAS-750 while running disk stress test
CSCuc05659	core.more files created in specific cases
CSCuc33140	SMB AO process is not getting killed while CIFS AO is enabled
CSCuc39607	filesystem_size_mismatch Alarm seen while downgrading
CSCud13729	HTTP Connections linger after running 'CONNECT' requests
CSCud29406	kernel msg "response: Error 2 cmd 3" observed in logs on occasion
CSCud56272	CM connectivity to WAE lost when Auto-Reg is disabled with preserve ip
CSCui82284	CM page loading issues in Chrome browser version - 29

Software Version 5.1.1 Command Changes

This section lists the new and modified commands in WAAS software version 5.1.1.

Table 2 lists the commands and options that have been added in WAAS version 5.1.1.

Table 2 CLI Commands Added in Version 5.1.1

Mode	Command	Description
EXEC	**copy scp**	Securely copies files from a source to a destination location, using the scp protocol.

Table 3 lists existing commands that have been modified in WAAS version 5.1.1.

Table 3 CLI Commands Modified in Version 5.1.1

Mode	Command	Description
EXEC	**copy sysreport**	Added the **scp** option to securely copy files.
	copy tech-support	Added the **scp** option to securely copy the technical support file.
	disk disk-name	Added the *diskxx* **enable force** option to reenable a defunct drive that was previously shut down.
	show cache http-metadatacache	Added the **sharepoint-prefetch** option to display Sharepoint statistics.
	show cifs	Added the **open-files** option to display open file information.
	show ssh	Removed support for SSH version 1.
	show statistics accelerator http	Added Sharepoint related fields to the output.
	traceroute	Added **tcp-syn** option to send TCP-SYN packets for trace routing instead of UDP.
	windows-domain	Removed the **findsmb**, **nmblookup**, **smbclient**, **smbstatus**, **smbtree**, **tdb-list**, **tdb-move**, **tdbbackup**, **tdbdump**, and **testparm** diagnostic options. Removed the **password** option for Windows domain join and leave options. Added the **organization-unit** option for Windows domain join. Added the **domain-controller**, **encryption-service**, **group**, **machine-account-info**, **user**, and **verify join** diagnostics options.
Global configuration	**accelerator cifs**	Added the **eviction-monitor**, **cumulative-time**, **duration**, and **enable** options to configure cache eviction monitoring.
	accelerator http	Added the **sharepoint-opt prefetch enable** option to enable Sharepoint prefetch optimization.
	no auto-register	Added the **preserve-ip** option.
	kerberos	Removed the **local-realm**, **realm**, and **server** options.
	sshd	Removed support for SSH version 1 and the **version** option to specify the SSH version to use, since only version 2 is supported.
	threshold-monitor	Changed the option name **asymmetric-flow-learn-failure** to **asymmetric-flow-query-failure**. Added the **accelerator cifs**, **directory resources**, **ff-average-local-response-time**, **ff-average-remote-response-time**, and **open-files** options to monitor the CIFS accelerator.
	windows-domain	Removed the **comment**, **realm**, **security ADS**, and **password-server** options. Added the **ldap-sign-and-seal enable** option to enable LDAP sign and seal service. Added the **machine-account-password lifespan** option to configure password settings and lifespan duration.

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*
- *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.

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