



# Release Notes for Cisco Wide Area Application Services Software Version 5.5.3

---

August 14, 2017



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:

- 5.5.3

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](http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html).

This Release Note contains the following sections:

- [New and Changed Features](#)
- [Interoperability and Support](#)
- [Upgrading from a Prerelease Version to Version 5.5.3](#)
- [Upgrading from a Release Version to Version 5.5.3](#)
- [Downgrading from Version 5.5.3 to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Operating Considerations](#)
- [Software Version 5.5.3 Resolved and Open Caveats, and Command Changes](#)
- [Cisco WAAS Documentation Set](#)
- [Obtaining Documentation and Submitting a Service Request](#)



# New and Changed Features

The following sections describe the new and changed features in Software Version 5.5.3:

- [Software Version 5.5.3 Filenames](#)
  - [Standard Image Files](#)
  - [No Payload Encryption Image Files](#)
- [Cisco WAAS Appliance System Firmware Update](#)
- [Cisco WAAS MAPI RPC over HTTP](#)
  - [Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP](#)
  - [Optimizing MAPI RPC over HTTPS](#)
  - [Cisco WAAS MAPI RPC over HTTP CLI Commands](#)
  - [MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP](#)
- [Supported Cisco WAAS Platforms for Akamai Caching](#)
- [Central Manager Support for TLSv1 Protocol for Communication with Registered Routers](#)

## Software Version 5.5.3 Filenames

This section describes the Cisco WAAS Software Version 5.5.3 software image files for use on Cisco WAAS appliances and modules and contains the following topics:

- [Standard Image Files](#)
- [No Payload Encryption Image Files](#)

## Standard Image Files

Cisco WAAS Software Version 5.5.3 includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- `waas-universal-5.5.3.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-5.5.3.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-5.5.3.x-k9.zip`—SM-SRE install .zip file that includes all the files necessary to install Cisco WAAS on the SM-SRE module.
- `ISR-WAAS-5.5.3.x.<build #>.ova` - ISR WAAS Release 5.3 files- 2500 Conns

The following additional files are also included:

- `waas-rescue-cdrom-5.5.3.x-k9.iso`—Cisco WAAS software recovery CD image.
- `waas-x86_64-5.5.3.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-5.5.3.x-k9.sysimg`—Flash memory recovery image for 32-bit platforms (all other devices).

- `waas-kdump-5.5.3.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-5.5.3.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 5.5.3 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-5.5.3.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-5.5.3.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-5.5.3.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.
- `Cisco-WAAS-vCM-100N-npe.ova` - VCM Release 5.5.3 NPE-100 Nodes
- `Cisco-WAAS-vCM-2000N-npe.ova` - VCM Release 5.5.3 NPE files -2000 Nodes
- `Cisco-WAAS-vWAAS-200-npe.ova` - VWAAS Release 5.5.3 NPE files-200 Conns
- `Cisco-WAAS-vWAAS-750-npe.ova` - VWAAS Release 5.5.3 NPE files -750 Conns
- `Cisco-WAAS-vWAAS-1300-npe.ova` - VWAAS Release 5.5.3 NPE files-1300 Conns
- `Cisco-WAAS-vWAAS-2500-npe.ova` - VWAAS Release 5.5.3 NPE files-2500 Conns
- `Cisco-WAAS-vWAAS-6000-npe.ova` - VWAAS Release 5.5.3 NPE files - 6000 Conns
- `Cisco-WAAS-vWAAS-12000-npe.ova` - VWAAS Release 5.5.3 NPE files-12000 Conns
- `Cisco-WAAS-vWAAS-50000-npe.ova` - VWAAS Release 5.5.3 NPE files- 50000 Conns
- `ISR-WAAS-5.5.3.x.<build #>-npe.ova` - ISR WAAS Release 5.5.3 NPE files- 2500 Conns

The following additional files are also included:

- `waas-rescue-cdrom-5.5.3.x-npe-k9.iso`—Cisco WAAS NPE software recovery CD image.
- `waas-x86_64-5.5.3.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-5.5.3.x-npe-k9.sysimg`—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- `waas-kdump-5.5.3.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-5.5.3.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](#). 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](#). The latest Baseboard Management Controller (BMC) firmware is required for Intelligent Platform Management Interface (IPMI) over LAN feature.
- RAID controller firmware on the WAE-674/7341/7371 and WAVE-7541/7571/8541—For details, see the [RAID Controller Firmware Update](#). 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](http://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-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-18a-18a-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—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](http://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-48a-48a-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-48a-48a-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 controller firmware for your hardware platform, which can be found on [cisco.com](http://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](http://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](http://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).

## Cisco WAAS MAPI RPC over HTTP

In Cisco WAAS v5.5.3, Cisco WAAS enables support for optimization of Microsoft Outlook and Microsoft Exchange traffic using Cisco WAAS MAPI RPC over HTTP and HTTPS protocol.

This section describes the following Cisco WAAS MAPI RPC over HTTP features:

- [Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP](#)
- [Optimizing MAPI RPC over HTTPS](#)
- [Cisco WAAS MAPI RPC over HTTP CLI Commands](#)
- [MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP](#)
  - [MAPI: Handled Traffic Pattern](#)
  - [MAPI: Connection Details](#)

## Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP

[Table 1](#) shows the clients and servers supporting WAAS MAPI RPC over HTTP:

**Table 1** *Clients and Servers Supporting WAAS MAPI RPC over HTTP*

Clients Supported	Servers Supported
Outlook 2013 (for Windows 7 and Windows 8)	Exchange 2013 (for Windows Server 2012, 2012 R2, 2008 R2 [full installation])

Clients Supported	Servers Supported
Outlook 2010 (for Windows 7 and Windows 8)	Exchange 2010 (for Windows Server 2012, 2012 R2, 2008, and 2008 R2)
Outlook 2007 (for Windows Vista, Windows 7)	

**Note**

If HTTP-AO or SSL-AO is disabled, the MAPI RPC over HTTP optimization feature will not work.

## Optimizing MAPI RPC over HTTPS

The WAAS software supports optimizing MAPI RPC over HTTPS, which allows the client and server to use the DCE/RPC protocol over an encrypted connection.

To support optimizing MAPI RPC over HTTPS, follow these steps:

- 
- Step 1** Configure SSL acceleration. For more information on configuring SSL acceleration, see the [“Configuring SSL Acceleration”](#) section of the *Cisco Wide Area Application Services Configuration Guide*.
- Step 2** When you configure SSL acceleration, be sure to enable protocol chaining, by checking the **Enable protocol chaining** check box on the SSL Accelerated Services window.

**Note**

If protocol chaining is not enabled, the WAAS device will only optimize SSL traffic on the specified IP address and port.

## Cisco WAAS MAPI RPC over HTTP CLI Commands

### New CLI Commands for MAPI RPC over HTTP

The following CLI commands have been added for Cisco WAAS MAPI RPC over HTTP.

- show statistics accelerator mapi
- show statistics accelerator mapi rpchttp

For a full description of these commands, see [Table 4](#) in the [Software Version 5.5.3 Command Changes](#) section.

### CLI Commands Modified for MAPI RPC over HTTP

The following CLI commands have been modified for Cisco WAAS MAPI RPC over HTTP.

- show accelerator mapi
- [no] debug accelerator mapi rpchttp

For a full description of these commands, see [Table 5](#) in the [Software Version 5.5.3 Command Changes](#) section.



## MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP

The MAPI Acceleration report displays MAPI acceleration statistics. For WAAS Version 5.5.3 and above, the following MAPI acceleration charts are added or modified:

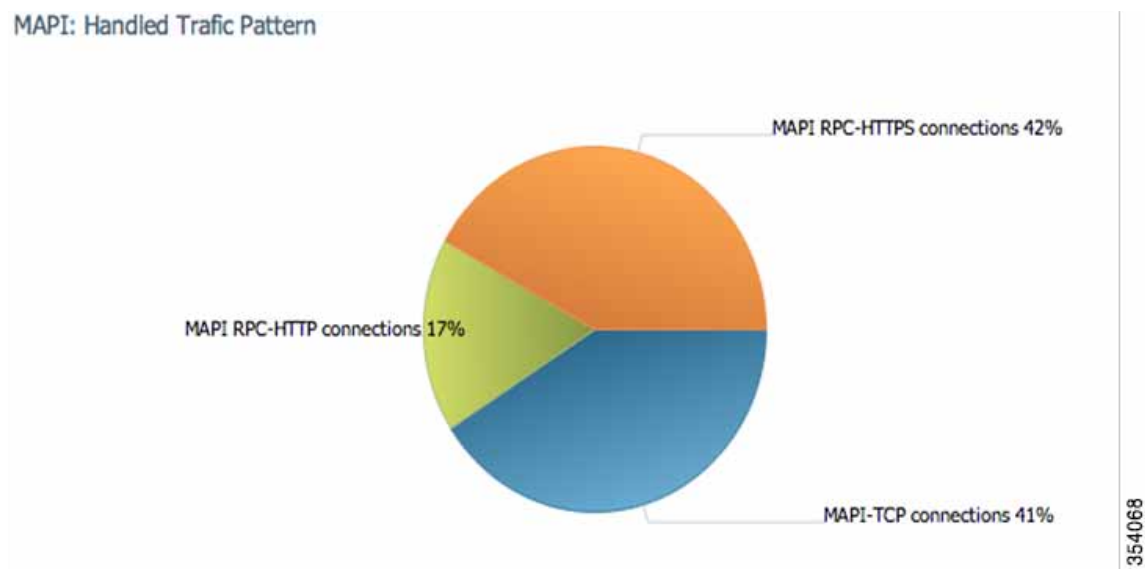
- [MAPI: Handled Traffic Pattern](#)—A new pie diagram that shows the three different types of traffic handled by the MAPI AO.
- [MAPI: Connection Details](#)—An existing chart for MAPI session connection statistics, MAPI: Connection Details now includes a new classification for optimized TCP and RPC HTTP(S) MAPI connections.

### MAPI: Handled Traffic Pattern

For WAAS Versions 5.5.3 and later, MAPI Acceleration reports include the MAPI: Handled Traffic Pattern pie chart. As shown in [Figure 1](#), this chart displays the percentage of three types of traffic:

- Total handled MAPI connections
- Total handled MAPI RPC HTTP connections
- Total handled MAPI RPC HTTPS connections

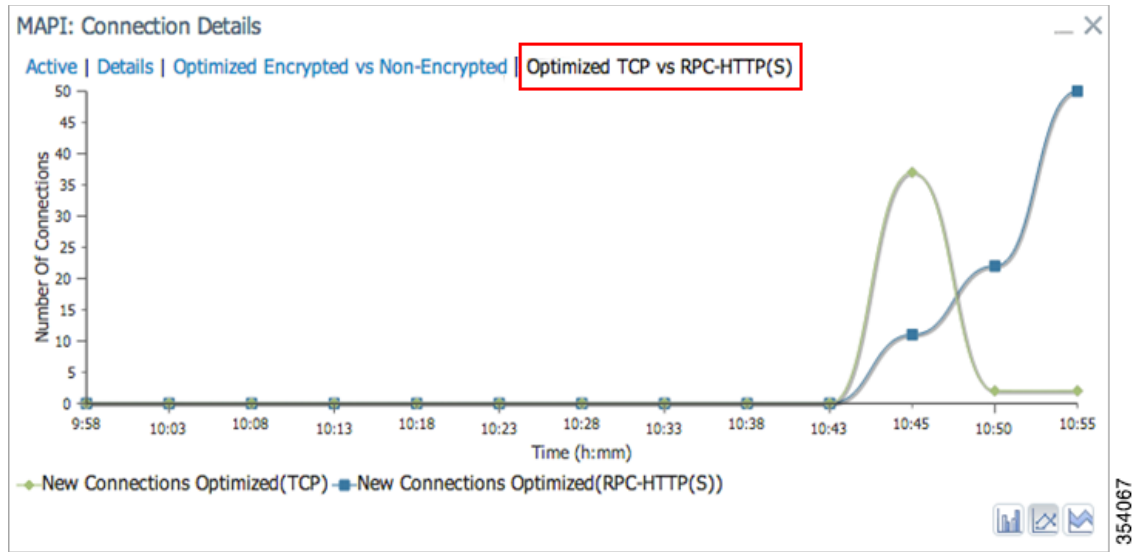
**Figure 1** Example of MAPI: Handled Traffic Pattern Chart



### MAPI: Connection Details

The MAPI Connection Details chart displays MAPI session connection statistics, showing the average number of active MAPI connections per device (at the device level, it shows the exact number for the last hour). In addition to information on newly handled MAPI connections, optimized connections, handed-off connections, dropped connections, and optimized vs. non-encrypted MAPI connections, WAAS Version 5.5.3 and later also provides information on optimized TCP vs. RPC HTTP(S) MAPI connections, as shown in [Figure 2](#).

Figure 2 Example of MAPI: Connection Details Chart



## Supported Cisco WAAS Platforms for Akamai Caching

Table 2 shows the supported Cisco WAAS Platforms for Akamai Caching for v5.5.3 and above.

Table 2 Supported Cisco WAAS Platforms for Akamai Caching

Appliance	Service Module	vWAAS	ISR-WAAS
WAVE-294	SM-700	vWAAS-200	ISR-WAAS-200 (ISR-4321)
WAVE-594	SM-900	vWAAS-750	ISR-WAAS-750 (ISR-4451, ISR-4431, ISR-4351, ISR-4331)
WAVE-694	SM-710	vWAAS-1300	ISR-WAAS-1300 (ISR-4451, ISR-4431)
	SM-910	vWAAS-2500	ISR-WAAS-2500 (ISR-4451)
		vWAAS-6000	



Warning

Although vWAAS-200 is supported on UCS-EN120E-208/K9, it cannot run Akamai Connect because this platform does not have enough storage to accommodate Akamai Connect object cache.

# Interoperability and Support


This section contains the following topics:

- [Hardware, Client, and Web Browser Support](#)
- [Cisco WAAS Version Interoperability](#)
- [AppNav Interoperability](#)
- [Cisco WAAS Express Interoperability](#)
- [WCCP Interoperability](#)
- [NTLM Interoperability](#)
- [Microsoft Windows XP Support](#)

## Hardware, Client, and Web Browser Support

[Table 3](#) lists the hardware, client, and web browser support for Cisco WAAS Software Version 5.5.3x.

**Table 3** *Hardware, CIFS Client, Web Browser Support*

Hardware support	<p>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.</p> <p> <b>Note</b> Some instances of SRE modules can experience communication problems with the router; this issue is tracked as CSCuu99817. If this scenario occurs, consider downgrading to WAAS Version 5.3.x.</p> <p>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 <a href="#">Cisco Wide Area Application Services vWAAS Installation and Configuration Guide</a>). You must deploy the Cisco WAAS Central Manager on a dedicated device.</p>
CIFS client support	<p>The Cisco WAAS software running on a branch WAE interoperates with these Common Internet File System (CIFS) clients: Windows 98/NT 4.0/2000/XP/Vista/7 and Windows Server 2003/2008 R2.</p>
Web browser support	<p>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.</p>

**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 5.5.3 devices with devices running earlier software versions:

- Cisco WAAS Version 5.5.3 is not supported running in a mixed version Cisco WAAS network where any Cisco WAAS device is running a software version earlier than 4.3.1. If you have any Cisco WAAS devices running a version earlier than 4.3.1, you must first upgrade them to version 4.3.1 (or a later version) before you install Version 5.5.3. 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 4.3.1 or later, you can begin the upgrade to Version 5.5.3 on the Central Manager. Directly upgrading a device from Version 4.0, 4.1, or 4.2 to 5.5.3 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.

**Caution**

When TCP traffic initiated by vulnerability assessment and security scanning tools goes through an AppNav IOM cluster, it may impair the functionality of the AppNav IOM module due to the structure of the packet. To ensure the functionality of the AppNav IOM module, we recommend that you prevent this traffic from being intercepted to the AppNav-IOM controller.

*To do this:* Place a WCCP redirect list to deny the traffic initiated from or targeted to the Security tools.

### 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

To avoid connection resets, Cisco recommends 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.

## WCCP Interoperability

Central Managers running Version 5.5.3x 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. For customers who have not upgraded to the latest Microsoft Windows OS, Cisco will continue to support Microsoft Windows XP with their Cisco WAAS deployments and customers may continue to obtain support from Cisco TAC for those Cisco WAAS deployments for six months after Microsoft's end-of-support date (Oct. 8, 2014).

## Upgrading from a Prerelease Version to Version 5.5.3

To upgrade from Cisco WAAS prerelease software to Version 5.5.3, 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 installation from the rescue CD or USB flash drive.

## Upgrading from a Release Version to Version 5.5.3

This section contains the following topics:

- [Upgrade Paths for WAAS Version 5.5.3](#)
- [Upgrading a Central Manager to Version 5.5.3](#)
- [Upgrading a WAAS System to Version 5.5.3](#)
- [Migrating a Central Manager from an Unsupported Platform](#)
- [Ensuring a Successful RAID Pair Rebuild](#)

For additional upgrade information and detailed procedures, refer to the [Cisco Wide Area Application Services Upgrade Guide](#).

## Upgrade Paths for WAAS Version 5.5.3

- Upgrading to Version 5.5.3 is supported only from Versions 4.3.x, 4.4.x, 4.5.x, 5.0.x, 5.1.x, 5.2.x, 5.3.x, and 5.4.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 5.5.3 version.
- Upgrading to Version 5.1.1 or later 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. Cisco WAAS Version 5.1 or later does not operate on these appliances. Upgrading a device group is not allowed if the group contains any of the unsupported devices. If you have a Central Manager running on one of these unsupported platforms, you can migrate it to a supported



platform by following the procedure in the [Migrating a Central Manager from an Unsupported Platform](#).

## Upgrading a Central Manager to Version 5.5.3

This section contains the following topics:

- [Central Manager Upgrade Guidelines](#)
- [Central Manager Upgrade and Interoperability](#)

### Central Manager Upgrade Guidelines

- 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.
- 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.

---

### Central Manager Upgrade and Interoperability

- 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.
- 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 5.5.3, 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 5.5.3, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.

## Upgrading a WAAS System to Version 5.5.3

This section contains the following topics:

- [WAAS System Upgrade Guidelines](#)
- [WAAS System Upgrade and Interoperability](#)

### WAAS System Upgrade Guidelines

- 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.
- 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](#).
- If you use the setup utility for basic configuration after upgrading to version 5.5.3, 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.
- 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](#).
- 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.



#### Note

If you upgrade from WAAS Version 5.3.5 to Version 5.5.x, the upgrade process resets SMB Settings values to their defaults. After you complete the upgrade, you must manually change the SMB Settings values to your custom settings.

To change the SMB Settings values:

1. Navigate to **Device Groups** > *device-group-name*.
2. Choose **Configure** > **Acceleration** > **SMB Settings**. The SMB Settings window is displayed.
3. Check or uncheck each SMB setting to fit the needs of your system.

For more information, see the section “Configuring SMB Acceleration” in the “Configuring Application Acceleration” chapter of the chapter in the [Cisco Wide Area Application Services Configuration Guide](#).

### WAAS System Upgrade and Interoperability

- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version.

- 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](#). If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.
- 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.
- 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.
- 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.
- 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.

- 
- 

## 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
```

## 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 5.5.3 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, 5.2.x, 5.3.x, and 5.4.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.
- 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 5.5.3 and contains the following topics:

- [Central Manager Report Scheduling](#)
- [Cisco WAAS Express Policy Changes](#)
- [Virtual Blade Configuration From File](#)
- [Using Autoregistration with Port-Channel and Standby Interfaces](#)
- [Disabling WCCP from the Central Manager](#)
- [Changing Device Mode To or From Central Manager Mode](#)
- [TACACS+ Authentication and Default User Roles](#)
- [Internet Explorer Certificate Request](#)
- [Default Settings with Mixed Versions](#)
- [Central Manager Support for TLSv1 Protocol for Communication with Registered Routers](#)

## 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.

## Central Manager Support for TLSv1 Protocol for Communication with Registered Routers

The WAAS Central Manager (version 5.5.3) uses one of the following protocols to communicate with its registered routers.

- TLSv1
- SSLv3

Depending on the router's version, the WAAS Central Manager decides which protocol version to use during the communication process.

As part of the poodle vulnerability fix, the following routers support the TLSv1 protocol and can be successfully registered with the WCM v 5.5.3.

- WAAS Express devices (version 15.5(02.06)T, 15.4(03)M02, 15.3(03)M05, 155-2.T, 15.5(01)T01). The hardware models 891, 19xx, 29xx, 39xx using WAAS Express version 15.3(03)M05, can be registered with the WCM, only from the WCM GUI.
- AppNav XE routers (version with poodle fix 3.10, 3.13, 3.14, 3.15. The ASR, CSR and ISR devices using AppNav XE version 3.13 (15.4-(3).S2) with poodle fix, can be registered with the WCM, only from the WCM GUI.



### Note

AppNav XE versions without the poodle fix can continue to communicate with the WCM (5.5.3 & lower version).

However, if you decide to upgrade the AppNav XE version to a version with the poodle fix, ensure that you upgrade the WCM to 5.5.3 so that it continues to communicate with the WAAS Central Manager.

For more information on the specific software versions with the poodle fix, please refer to CSCur43251.

## Software Version 5.5.3 Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, command changes, and other changes in Software Version 5.5.3 and contains the following topics:

- [Software Version 5.5.3 Resolved Caveats](#)
- [Software Version 5.5.3 Open Caveats](#)
- [Software Version 5.5.3 Command Changes](#)
- [Using Previous Client Code](#)

## Software Version 5.5.3 Resolved Caveats

The following caveats were resolved in Software Version 5.5.3.

Caveat ID Number	Headline
<a href="#">CSCuq50575</a>	WAAS Admin Certificate reverts to self-signed cert after httpd restart
<a href="#">CSCur71633</a>	Copying files with SMB Ext attributes using cmd fails with SMB-AO
<a href="#">CSCur88133</a>	SMBAO core file generated on WAAS
<a href="#">CSCus39181</a>	To offload SMB-AO when SMB Metadata Cache reaches Max limit
<a href="#">CSCus57999</a>	Topology view is empty or incomplete
<a href="#">CSCus64724</a>	Empty Response on Dual -Sided Setup
<a href="#">CSCus70116</a>	WAASX device not coming to online after register with WCM
<a href="#">CSCus73812</a>	Likewise Core, when selecting DC list (failing over DC in AD)
<a href="#">CSCus82405</a>	EMAPI support for WIN2012R2 by enabling Recycle Bin Option in waas DC
<a href="#">CSCus87492</a>	CM very slow and devices offline in a particular situation
<a href="#">CSCut49148</a>	WAAS / Prime Integration broken after POODLE Patch
<a href="#">CSCus85330</a>	WAAS Device Reload with certain type of traffic

## Software Version 5.5.3 Open Caveats

The following caveats are open caveats for Software Version 5.5.3.

Caveat ID Number	Headline
<a href="#">CSCuv79705</a>	All devices in pending/offline state in WAAS CM after 5.5.3 upgrade
<a href="#">CSCuu18109</a>	WAAS vCM in non-working condition after 5.5.3 code upgrade
<a href="#">CSCuu99817</a>	SRE module fails to communicate with router
<a href="#">CSCut27741</a>	Current active optimized flow exceeds connection limit
<a href="#">CSCut49901</a>	Rpchtts fails to connect due to missing out channel in 2nd pair

## Software Version 5.5.3 Command Changes

This section lists the new and modified commands in WAAS Software Version 5.5.3.

**Table 4** *CLI Commands Added in Version 5.5.3*

Mode	Command	Description
EXEC	<b>show statistics accelerator mapi</b>	The following counters are added to this command's output: <ul style="list-style-type: none"> <li>• Total Handled RPC TCP Connections</li> <li>• Total Handled RPCH HTTP Connections</li> <li>• Total Handled RPCH HTTPS Connections</li> <li>• Total Optimized RPC TCP Connections</li> <li>• Total Optimized RPCH HTTP Connections</li> <li>• Total Optimized RPCH HTTPS Connections</li> <li>• Total Handled RPCH Virtual Sessions</li> <li>• Total Optimized RPCH Virtual Sessions</li> <li>• Total Pipe-Through Virtual Sessions</li> </ul>
EXEC	<b>show statistics accelerator mapi rpchttp</b>	Shows statistics related to MAPI RPC over HTTP optimization details. The output includes statistics about MAPI RPC over HTTP connections, debugging details, and analysis-supported statistics.

**Table 5** *CLI Commands Modified in Version 5.5.3*

Mode	Command	Description
EXEC	<b>show accelerator mapi</b>	Added accelerator configuration details about MAPI RPC over HTTP.
EXEC	<b>[no] debug accelerator mapi rpchttp</b>	Added logging for RPC HTTP module in MAPI-AO.

## Using Previous Client Code

If you have upgraded to Cisco WAAS Version 5.5.3 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/CADDBBeanTemplateHeader.xsl
org/apache/axis2/schema/template/CADDBBeanTemplateSource.xsl
org/apache/axis2/schema/template/PlainBeanTemplate.xsl
org/apache/axis2/schema/template/ADDBBeanTemplate.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 `ADDBBeanTemplate.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() && !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](#)
- [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 “[Cisco WAAS Documentation Set](#)” section.

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

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

© 2015 Cisco Systems, Inc. All rights reserved.

