



Release Note for Cisco Wide Area Application Services Software Version 6.2.1x

February 20, 2019



Note

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

Contents

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

- 6.2.1x

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.

This Release Note contains the following sections:

- [New and Changed Features](#)
- [Interoperability and Support](#)
- [Upgrading from a Prerelease Version to Version 6.2.1x](#)
- [Upgrading from a Release Version to Version 6.2.1x](#)
- [Downgrading from Version 6.2.1x to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Operating Considerations](#)
- [Software Version 6.2.1x 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 6.2.1x:

- [Cisco Software Version 6.2.1x New and Changed Features](#)
- [Cisco Software Version 6.2.1x Filenames](#)
- [Cisco WAAS Appliance System Firmware Update](#)

Cisco Software Version 6.2.1x New and Changed Features

Cisco WAAS Software Version 6.2.1 includes the following new features and changes:

- Cisco WAAS Version 6.2.1 with Akamai Connect Version 1.4:
 - Supported WAAS platforms for Akamai Connect connection counts scale beyond 6,000 connections, to scale close to the connection limit on WAAS mid- to high-end platforms.
 - HAR (HTTP Archive format) file support—Support for generating HAR files on both LAN and WAN sides, with filter support. Although not fully integrated with the WAAS CM and WAAS CLI, you can use the **script execute harcap.sh** to launch and manage this feature.
 - Prepositioning proxy support—Akamai Connect utilizes a non-transparent proxy for prepositioning content.
 - Prepositioning User Agent—Provides information on client browser and operating system type used to access the URLs specified for a preposition task.
 - Force IMS—Akamai Connect supports an additional force refresh option for dual-sided deployments with filtering/SWG/CWS servers up stream.
 - Prepositioning of JNLP (Java Network Launch Protocol) files, which contain URL references for Java Web Start.
 - Prepositioning of HLS (HTTP Live Streaming) and HDS (HTTP Dynamic Streaming) video manifest files.
 - Enhancements to OTT caching, including query formulation and support for YouTube R playback with range requests.
- vWAAS new and changed features:
 - Cisco vWAAS on RHEL KVM
 - EzDeploy script for simplified deployment of vWAAS on RHEL KVM
 - L2 Inline traffic interception for vWAAS on RHEL KVM
 - vWAAS on Microsoft Azure
 - For vWAAS-12000 and vWAAS-50000, Akamai Connect connection counts scale beyond 6,000 connections, to scale close to the WAAS connection limit for these models.
 - vWAAS-150 supported for Microsoft Hyper-V and RHEL KVM
- Office 365 optimization support
- SMART-SSL acceleration for YouTube, (TM) traffic. SMART-SSL is an encryption service that enables L7 application network services (e.g. ftp, http, dns) to optimize traffic on SSL/TLS encrypted connections. This feature is optional and therefore disabled by default. If you would like to learn more about this, please refer to [Configuring SMART-SSL Acceleration](#).
- SMB content prepositioning support.

- Cisco WAAS support for L7 optimization of encrypted SMB traffic.
- Cisco WAAS support for L7 optimization of RPCHTTP(S) traffic.
- For a list of CLI commands added to or changed for WAAS Version 6.2.1x, see [Cisco Software Version 6.2.1x Command Changes](#).

Cisco Software Version 6.2.1x Filenames

This section describes the Cisco WAAS Software Version 6.2.1x software image files for use on Cisco WAAS appliances and modules and contains the following topics:

- [Standard Image Files](#)
- [No Payload Encryption Image Files](#)
- For a list of vWAAS image files, see “OVA Files for vWAAS Models” in Chapter 1, “Introduction to vWAAS” in the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

Standard Image Files

Cisco WAAS Software Version 6.2.1x includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- `waas-universal-6.2.1.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-6.2.1.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.

The following additional files are also included:

- `waas-rescue-cdrom-6.2.1.x-k9.iso`—Cisco WAAS software recovery CD image.
- `waas-x86_64-6.2.1.x-k9.sysimg`—Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- `waas-6.2.1.x-k9.sysimg`—Flash memory recovery image for 32-bit platforms (all other devices).
- `waas-kdump-6.2.1.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-6.2.1.x.zip`—Contains the alarm and error message documentation.

No Payload Encryption Image Files

Cisco WAAS Software Version 6.2.1x 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-6.2.1.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-6.2.1.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-6.2.1.x-npe-k9.zip`—SM-SRE install .zip file that includes all the NPE files necessary to install Cisco WAAS on the SM-SRE module.

The following additional files are also included:

- `waas-rescue-cdrom-6.2.1.x-npe-k9.iso`—Cisco WAAS NPE software recovery CD image.
- `waas-x86_64-6.2.1.x-npe-k9.sysimg`—Flash memory NPE recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- `waas-6.2.1.x-npe-k9.sysimg`—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- `waas-kdump-6.2.1.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-6.2.1.x-npe.zip`—Contains the NPE alarm and error message documentation.

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.

This section contains the following topics:

- [BIOS Update](#)
BIOS on the WAVE-294/594/694/7541/7571/8541 models. The latest BIOS is required for AppNav operation.
- [BMC Firmware Update](#)
BMC firmware on the WAVE-294/594/694/7541/7571/8541 models. The latest BMC (Baseboard Management Controller) firmware is required for Intelligent Platform Management Interface (IPMI) over LAN feature.
- [RAID Controller Firmware Update](#)
RAID controller firmware on the WAVE-7541/7571/8541. The latest RAID (Redundant Array of Independent Disks) 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.

For the specific BIOS version required for WAVE-594/694 models, WAVE-7541/7571/8541 models, and WAVE-294 models, please see the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page ([registered](#) customers only).

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 last three characters of the Version value, for example, “20a,” show the BIOS version installed on the device.

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

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

```
copy ftp install ip-address remotefiledir waas-bios-installer-20a-19a-13a-k9.bin
```

Use the appropriate BIOS installer file for your appliance model.

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

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

BMC Firmware Update

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

- WAVE-294/594/694—49a
- WAVE-7541/7571/8541—27a

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

To determine if you are running the correct firmware version, use the **show bmc info** command. The following example displays the latest BMC firmware version installed on the device (49a here):

```

wave# show bmc info
Device ID           : 32
Device Revision     : 1
Firmware Revision   : 0.49                <<<<< version 49
IPMI Version        : 2.0
Manufacturer ID     : 5771
Manufacturer Name   : Unknown (0x168B)
Product ID          : 160 (0x00a0)
Product Name        : Unknown (0xA0)
Device Available    : yes
Provides Device SDRs : no
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
Aux Firmware Rev Info :
    0x0b
    0x0c
    0x08
    0x0a                <<<<< a
.
.
.

```

If a BMC firmware update is needed, you can download it from cisco.com at the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page (registered customers only). For example, if the firmware binary image is named `waas-bmc-installer-49a-49a-27a-k9.bin`, you can use the following command to update the firmware from the image file that is available through FTP on your network:

```
copy ftp install ip-address remotefiledir waas-bmc-installer-49a-49a-27a-k9.bin
```

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

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

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

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

RAID Controller Firmware Update

We recommend that you upgrade to the latest RAID-5 controller firmware for your hardware platform, which can be found on cisco.com at the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page (registered customers only). The firmware differs depending on your hardware platform:

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

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

Interoperability and Support

This section contains the following topics:


- [Hardware, Client, and Web Browser Support](#)
- [Cisco WAAS Version Interoperability](#)
- [Cisco WAAS and vWAAS Interoperability](#)
- [Cisco WAAS, ISR-WAAS and IOS-XE Interoperability](#)
- [Cisco AppNav and AppNav-XE Interoperability](#)
- [Cisco WAAS, ASR/CSR, and IOS-XE Interoperability](#)
- [Cisco WAAS Express Interoperability](#)
- [Traffic Interception Interoperability](#)
- [NTLM Interoperability](#)
- [Microsoft Windows XP Support Notice](#)
- [Citrix ICA Interoperability](#)

Hardware, Client, and Web Browser Support

[Table 1](#) lists the hardware, client, and web browser support for Cisco WAAS Software Version 6.2.1x.

Table 1 *WAAS 6.2.1x Hardware, Client and Web Browser Support*

Hardware support	<p>The Cisco WAAS software operates on these hardware platforms:</p> <ul style="list-style-type: none"> • WAVE-294, 594, 694, 7541, 7571, 8541 <p><i>Consider the following if you upgrade a WAVE-694 from WAAS Version 5.x to Version 6.x, and the WAVE-694 has the following parameters:</i></p> <ul style="list-style-type: none"> – 24 GB RAM – You have used the <code>disk object-cache extend</code> command before the upgrade. <p>After the upgrade from WAAS Version 5.x to 6.x, you may see the disk_full alarm. (For more information on alarms, see of the WAAS Alarm Book.)</p> <p>To address the above scenario, follow these steps <i>before</i> beginning the upgrade process:</p> <ol style="list-style-type: none"> a. Use the no disk object-cache extend command to disable the disk object cache extend command. b. Reload the WAVE-694 in WAAS Version 5.x. c. Verify that the device is operational. d. Upgrade from WAAS Version 5.x to WAAS Version 6.x. <ul style="list-style-type: none"> • SM-SRE-700/710, 900/910 • ISR-WAAS-200, 750, 1300, 2500 • vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000 on ESXi. For information on minimum ESXi version supported for each vWAAS model, see “Requirements for Cisco vWAAS” in Chapter 1, “Introduction,” in the Cisco Virtual Wide Area Application Services Installation and Configuration Guide. • vWAAS-150, vWAAS-200, 750, 1300, 2500, 6000, 12000, 50000 on Microsoft Hyper-V. For information on the version of Windows supported for each vWAAS model on Microsoft Hyper-V, see “Platforms Supported for vWAAS on Hyper-V” in Chapter 5, “vWAAS on Hyper-V” in the Cisco Virtual Wide Area Application Services Installation and Configuration Guide. • For WAAS Version 6.2.1 and later, vWAAS is supported on RHEL KVM and Microsoft Azure. <p>For information on vWAAS for RHEL KVM, see Chapter 2, “Installing Cisco vWAAS” in the Cisco Virtual Wide Area Application Services Installation and Configuration Guide.</p> <p>For information on vWAAS on Microsoft Azure, see Chapter 5, “Cisco vWAAS on Microsoft Hyper-V” in the Cisco Virtual Wide Area Application Services Installation and Configuration Guide.</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 5.0.x or later is required on the data center side).</p> <p>You must deploy the Cisco WAAS Central Manager on a dedicated device.</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.</p> <ul style="list-style-type: none"> For WAAS version 5.4.1 and later, you are no longer prompted to install the Google Frame plug-in when you access the Central Manager GUI using Internet Explorer. However, if Google Frame plug-in has already been installed earlier, IE will continue using it. 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 will not display. <p> Note A known issue in Chrome Version 44.0 may prevent some WAAS CM pages—including Device Listing, Reports, Software Update pages—from loading properly. In Chrome Version 43.0 all WAAS CM pages work as expected.</p>
---------------------	--

Cisco WAAS Version Interoperability

Consider the following guidelines when operating a Cisco WAAS network that mixes Software Version 6.2.1x devices with devices running earlier software versions:

- **Cisco WAAS CM interoperability:**

In a mixed version Cisco WAAS network, the Central Manager must be running the highest version of the Cisco WAAS software, and associated Cisco WAAS devices must be running Version 5.0.1 or later.

- **Cisco WAAS system interoperability:**

Cisco WAAS Version 6.2.1x is not supported running in a mixed version Cisco WAAS network in which any Cisco WAAS device is running a software version earlier than Version 5.0.x. Directly upgrading a device from a version earlier than Version 5.0.x to 6.2.1x is not supported.

Cisco WAAS and vWAAS Interoperability

Consider the following guidelines when using Cisco vWAAS with WAAS:

- For vWAAS with WAAS Version 6.1.x and later, the vWAAS and vCM devices require *both* virtual (network) interfaces to be present, but both need not be active. If only one virtual interface is active, the vWAAS and vCM devices will not be operational after power up. For more information, see “Configuring vWAAS” in the *Configuring Cisco vWAAS and Viewing vWAAS Components* chapter of the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

**Note**

When selecting the format in the vSphere Client for the virtual machine's disks for vWAAS with VMware vSphere ESXi, you must choose the **Thick Provision Eager Zeroed** disk format for vWAAS deployment; this is the format recommended with vWAAS deployment for a clean installation.

- For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.

**Note**

When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and diskless mode.

- If the virtual host was created using an OVA file of vWAAS for WAAS Version 5.0 or earlier, and you have upgraded vWAAS within WAAS, you must verify that the SCSI Controller Type is set to **VMware Paravirtual**. Otherwise, vWAAS will boot with no disk available and will fail to load the specified configuration.

If needed, change the SCSI controller type to **VMware Paravirtual** by following these steps:

- a. Power down the vWAAS.
- b. From the VMware vCenter, navigate to **vSphere Client > Edit Settings > Hardware**.
- c. Choose **SCSI controller 0**.
- d. From the Change Type drop-down list, verify that the SCSI Controller Type is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.
- e. Click **OK**.
- f. Power up the vWAAS, with WAAS Version 6.1.x or later.

For more information on setting the SCSI Controller Type and on the vWAAS VM installation procedure, see Chapter 2, “Installing Cisco vWAAS” section “Installing the vWAAS VM” in the [Cisco Virtual Wide Area Application Services Installation and Configuration Guide](#).

Cisco WAAS, ISR-WAAS and IOS-XE Interoperability

Table 2 shows Cisco WAAS, ISR-WAAS and IOS-XE Interoperability.

Table 2 Cisco WAAS, ISR-WAAS and IOS-XE Interoperability

ISR-Platform	Minimum ISR-WAAS Version	Minimum IOS-XE Version
ISR-4451	5.2.1	3.10
ISR-4431, 4351, 4331, 4321	5.4.1	3.13

**Note**

ISR4321-B/K9 is not supported for ISR-WAAS installation.

Cisco AppNav and AppNav-XE Interoperability

Consider the following guidelines when deploying the Cisco AppNav solution, for AppNav and AppNav-XE.

- 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.



Note WAAS Version 6.1.x and later does not support AppNav IOM.

- All AppNav devices in a single cluster must be of the same exact type. This includes IOS-XE devices, down to memory and ESP configuration.
 - All Cisco ASRs (Aggregation Services Routers) in an AppNav Controller Group need to be the same model, with the same ESP (Embedded Services Processor) rate (in Gbps). For example, in an AppNav Controller Group, you cannot have one ASR-1006 40-Gbps ESP and one ASR-1006 100-Gbps ESP.
 - The same principle is true for using the ISR (Integrated Services Router) 4000 series. You cannot have an ISR-4451 and an ISR-4321 in the same AppNav-XE cluster.
- 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.



Note 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, ASR/CSR, and IOS-XE Interoperability

Table 3 shows Cisco WAAS, ASR/CSR and IOS-XE Interoperability.

Table 3 *Cisco WAAS, ASR/CSR, and IOS-XE Interoperability*

WAAS Version	ASR/CSR Series	IOS-XE Version Supported
5.2.1	ASR-1000x/CSR-1000V	3.9
5.3.1, 5.3.3, 5.3.5a	ASR-1000x/CSR-1000V	3.9-3.12
5.3.5f	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
5.4.x	ASR-1000x/CSR-1000V	3.13
5.5.1	ASR-1000x/CSR-1000V	3.13-3.15
5.5.3	ASR-1000x/CSR-1000V	3.13-3.16
5.5.5,x	ASR-1000x/CSR-1000V	3.13-3.17

WAAS Version	ASR/CSR Series	IOS-XE Version Supported
6.1.1a	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
6.2.1x	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17

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

If you are upgrading the WAAS Express devices to IOS 15.3(3)M image, as part of the new AppX/K9 (Application Experience) license support in WAAS Express IOS 15.3(3)M images, you need to upgrade the WAAS Central Manager to WAAS v5.3.1 or later, or else the devices will go offline.



Note

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

Table 4 lists the Cisco WAAS, WAAS Express and IOS Interoperability

Table 4 Cisco WAAS, WAAS Express and IOS Interoperability

WAAS Version	WAAS Express Platform	IOS Version Supported
5.2.1	89x,19xx, 29xx, 39xx	15.2(4)M, 15.3(1)T
5.3.1 5.3.5x 5.4.1 5.5.x 6.1.x 6.2.1x	89x,19xx, 29xx, 39xx	15.2(4)M, 15.3(1)T, 15.3(3)M, 15.4(2)T, 15.5(1)T, 15.5(2)T, 15.5(3)M, 15.6(1)T, 15.6(2)T



Note

39xxE series routers do not support WAAS Express.

Traffic Interception Interoperability

This section contains the following topics:

- [General Traffic Interception Interoperability](#)
- [WCCP Interoperability](#)

General Traffic Interception Interoperability

Cisco WAAS uses the following traffic interception methods: Web Cache Communications Protocol (WCCP), WCCP Version 2, AppNav, Inline, Policy-Based Routing (PBR) and ITD (advanced version of PBR). For WAAS Version 5.5.1 and earlier, WAAS supports WCCP, AppNav, and vPATH.

Consider the following guidelines when configuring traffic interception for Cisco WAAS.

- ISR-WAAS devices support only the AppNav Controller interception method. For more information on AppNav, see [Cisco AppNav and AppNav-XE Interoperability](#).
- For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.
- Pass-through traffic does not benefit from optimization. For example, SSH port 22 has minimal traffic volume, so would not benefit by optimizing TCP flows.

For more information on traffic interception methods, see the “Configuring Traffic Interception” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

WCCP Interoperability

Central Managers running Version 6.2.1x can manage WAEs running WAAS Version 5.x and later. However, we recommend that all WAEs in a given WCCP service group be running the same WAAS 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 Version 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 “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 Notice

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).

Citrix ICA Interoperability

Citrix ICA versions 7.x (XenApp and XenDesktop) contain changes affecting the optimization efficiency of WAAS compared to that achieved with Citrix ICA versions 6.x. To maximize the effectiveness of WAAS, the Citrix administrator should configure the following:

Adaptive Display: Disabled

Legacy Graphic Mode: Enabled

Upgrading from a Prerelease Version to Version 6.2.1x

To upgrade from Cisco WAAS prerelease software to Version 6.2.1x, 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 6.2.1x

Upgrading to WAAS Version 6.2.1xx is supported from WAAS Version 4.2.1 and later. For information on upgrade paths, see [Upgrade Paths and Considerations for Version 6.2.1x](#).

To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version. For an overview of the upgrade process from a release version to Version 6.2.1xx, see [Workflow: Upgrading from a Release Version to Version 6.2.1x](#).

This section contains the following topics:

- [Upgrade Paths and Considerations for Version 6.2.1x](#)
- [Workflow: Upgrading from a Release Version to Version 6.2.1x](#)
 - [Upgrade Part 1: Create a Backup of the Primary WAAS CM Database](#)
 - [Upgrade Part 2: Upgrade the Standby WAAS CM](#)
 - [Upgrade Part 3: Upgrade the Primary WAAS CM](#)
 - [Upgrade Part 4: Upgrade the Branch WAE Devices](#)

- Upgrade Part 5: Upgrade the Data Center WAAS Software
- Upgrade Part 6: Upgrade Each Data Center WAE
- Upgrade Part 7: WCCP and Migration Processes
- Upgrade Part 8: Post-Upgrade Tasks
- Migrating a WAAS CM from an Unsupported to a Supported Platform
- Migrating a Physical Appliance Being Used as a WAAS CM to a vCM
- 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 and Considerations for Version 6.2.1x

This section contains the following topics:

- Upgrade Paths for WAAS Version 6.2.1x
- Upgrading from Cisco WAAS Version 5.x and Later to Version 6.2.1x
- Upgrading from Cisco WAAS Version 4.2.x to Version 6.2.1x

Upgrade Paths for WAAS Version 6.2.1x

As shown in [Table 5](#), upgrading to WAAS Version 6.2.1x is supported from WAAS Version 4.2.x and later.

- You can upgrade directly to WAAS Version 6.2.1x from WAAS versions 5.5.x, 6.0.x, and 6.1.1x.
- To upgrade to WAAS Version 6.2.1x from a WAAS version earlier than 5.5.x, you must first upgrade the device to WAAS Version 5.5.x or later, and from one of these versions, upgrade to Version 6.2.1x.

Table 5 Upgrade Paths to WAAS Version 6.2.1x

Current WAAS Version	WAAS CM Upgrade Path	WAAS Upgrade Path
5.5.3 and later	<ul style="list-style-type: none"> • Upgrade directly to 6.2.1x 	<ul style="list-style-type: none"> • Upgrade directly to 6.2.1x
4.3.x through 5.5.1	<ol style="list-style-type: none"> 1. Upgrade to 5.5.3 2. Upgrade to 6.2.1x 	<ol style="list-style-type: none"> 1. Upgrade to 5.5.3 2. Upgrade to 6.2.1x
4.2.x	<ol style="list-style-type: none"> 1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3 3. Upgrade to 6.2.1x 	<ol style="list-style-type: none"> 1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3 3. Upgrade to 6.2.1x

Upgrading from Cisco WAAS Version 5.x and Later to Version 6.2.1x

Consider the following guidelines when upgrading from Cisco WAAS Version 5.x to Version 6.2.1x.

**Note**

When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and diskless mode.

- 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 5.2 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.

- 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 CMS (Centralized Management System) logs.

Upgrading from Cisco WAAS Version 4.2.x to Version 6.2.1x

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. For more information on upgrade paths, see [Table 5](#).

Workflow: Upgrading from a Release Version to Version 6.2.1x

To upgrade from a Release Version to Version 6.2.1x, complete the tasks listed in [Table 6](#).

Table 6

Workflow: Upgrading from a Release Version to Version 6.2.1x

Workflow Task	Description
<ul style="list-style-type: none"> Upgrade Part 1: Create a Backup of the Primary WAAS CM Database 	<ul style="list-style-type: none"> Before you start the upgrade process from a release version to Version 6.2.1x, create a backup of the primary WAAS CM database and save it to a remote location.
<ul style="list-style-type: none"> Upgrade Part 2: Upgrade the Standby WAAS CM 	<ul style="list-style-type: none"> If your WAAS system has a standby WAAS CM, upgrade the standby WAAS CM before you upgrade the primary WAAS CM.
<ul style="list-style-type: none"> Upgrade Part 3: Upgrade the Primary WAAS CM 	<ul style="list-style-type: none"> Upgrade the primary WAAS CM, including verifying that the new WAAS image is loaded correctly, verifying connectivity between WAAS CM and branch WAE devices, and verifying that all WAE devices are online.
<ul style="list-style-type: none"> Upgrade Part 4: Upgrade the Branch WAE Devices 	<ul style="list-style-type: none"> Upgrade the branch WAE devices, including verifying that new WAAS image is loaded correctly, verifying that correct licenses are installed, and saving the new configuration.
<ul style="list-style-type: none"> Upgrade Part 5: Upgrade the Data Center WAAS Software 	<ul style="list-style-type: none"> Upgrade the data center WAAS software, including upgrading each data center WAE device.
<ul style="list-style-type: none"> Upgrade Part 6: Upgrade Each Data Center WAE 	<ul style="list-style-type: none"> Upgrade each data center WAE device, including disabling and re-enabling WCCP
<ul style="list-style-type: none"> Upgrade Part 7: WCCP and Migration Processes 	<ul style="list-style-type: none"> For information on the sets of tasks to enable and reconfigure WCCP, and information on configuring accelerators, switches and routers for migration, see the <i>Cisco Wide Area Application Services Upgrade Guide</i>.
<ul style="list-style-type: none"> Upgrade Part 8: Post-Upgrade Tasks 	<ul style="list-style-type: none"> After you complete the WAAS system upgrade to Version 6.2.1x, perform tasks including clearing your browser cache, verifying licenses, and verifying proper configuration of applications accelerators, policies, and class maps.

Upgrade Part 1: Create a Backup of the Primary WAAS CM Database

Before upgrading to WAAS Version 6.2.1x, create a backup of the WAAS CM database.



Caution

If you are upgrading your Virtual WAAS CM from an earlier WAAS version to WAAS Version 6.2.1x, **it is crucial that you create a backup of the WAAS CM database and save it to an external file (FTP/SFTP) before you upgrade to WAAS Version 6.2.1x.** The upgrade process on this type of configuration will automatically clear system and data partition, which will erase the WAAS CM database.

If you upgrade the vCM device to WAAS Version 6.2.1x via the console, a warning message similar to the following will be displayed:

```
WARNING: Upgrade of vCM device to 6.2.0 (or) higher version with '/sw' and '/swstore'
```

size less than 2GB will clear system and data partition.

If you upgrade the vCM device to WAAS Version 6.2.1x via the GUI, a warning message is not displayed.

After upgrade is complete, restore the saved WAAS CM database to your system.

Follow these steps to create a backup of the WAAS CM database:

Step 1 Telnet to the primary WAAS CM, using the **telnet** command:

```
telnet cm ip-address
```

Step 2 Create the database backup, using the **cms database backup** command:

```
waas-cm# cms database backup
```

Step 3 The **cms database backup** command displays the following information:

```
creating backup file with label 'backup'
backup file local1/filename filedate.dump is ready. use 'copy' command to move the backup
file to a remote host.
```

Step 4 Copy the backup database file to a remote location, using the **copy disk** command:

```
waas-cm# copy disk ftp hostname ip-address remotefiledir remotefilename localfilename
```

Step 5 Verify that the backup file was copied correctly by verifying file size and time stamp.

Upgrade Part 2: Upgrade the Standby WAAS CM

Follow these steps to upgrade the standby WAAS CM, if present in your WAAS system.

Step 1 Telnet to the standby WAAS CM IP address:

```
telnet standby-cm-ip-address
```

Step 2 Copy the new software image to the standby WAAS CM, using the **copy ftp** command:

```
wae# copy ftp install ftpserver / waas-image.bin
```



Note This example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.

Step 3 Reload the standby WAAS CM, using the **reload** command

Step 4 Verify that the new image is loaded correctly, using the **show version** command.

Step 5 To confirm connectivity, ping the primary WAAS CM and branch WAE devices.

Step 6 Wait at least five minutes.

Step 7 To ensure that the database has been synchronized, confirm the database last synchronization time, using the **show cms info** command.

Step 8 From the primary WAAS CM, confirm that the status indicator for the standby WAAS CM is online and green.

Upgrade Part 3: Upgrade the Primary WAAS CM

Perform the following tasks *before* you upgrade the primary WAAS CM:

- Before upgrading the primary WAAS CM, create a backup copy of the primary WAAS CM database. For more information, see [Upgrade Part 1: Create a Backup of the Primary WAAS CM Database](#).
- If your WAAS system has a standby WAAS CM, you must upgrade the standby WAAS CM before you upgrade the primary WAAS CM. For more information, see [Upgrade Part 2: Upgrade the Standby WAAS CM](#).

Follow these steps to upgrade the primary WAAS CM.

Step 1 Telnet to the primary WAAS CM IP address:

```
telnet primary-cm-ip-address
```

Step 2 Copy the new Version 6.2.1x software image to the primary WAAS CM, using the **copy ftp** command:

```
wae# copy ftp install ftpserver / waas-image.bin
```



Note This example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.

Step 3 Reload the primary WAAS CM, using the **reload** command

Step 4 Verify that the new Version 6.2.1x image is loaded correctly, using the **show version** command.

Step 5 To confirm connectivity, ping the standby WAAS CM (if present in your WAAS system) and branch WAE devices.

Step 6 Confirm that the CMS services are running, using the **show cms info** command.

Step 7 Choose **Devices > All Devices** and verify that all WAE devices are online.

Step 8 Choose Device Groups > AllWAASGroups > Assign Devices and verify that each WAE device is listed with a green check mark.

Upgrade Part 4: Upgrade the Branch WAE Devices

Before you upgrade the upgrade the branch WAE devices, verify that you have completed the following tasks:

- Created a backup copy of the primary WAAS CM database. For more information, see [Upgrade Part 1: Create a Backup of the Primary WAAS CM Database](#).
- Upgraded the standby WAAS CM, if one is present on your WAAS system. For more information, see [Upgrade Part 2: Upgrade the Standby WAAS CM](#).
- Upgraded the primary WAAS CM. For more information, see [Upgrade Part 3: Upgrade the Primary WAAS CM](#).

Follow these steps to upgrade the branch WAE devices.

Step 1 Access the primary WAAS CM GUI:

```
https://cm-ip-address
```

- Step 2** Verify that all WAE devices are online (displaying green).
- Step 3** Resolve any alarm conditions that may exist.
- Step 4** Open a console session or Telnet to the branch WAE.
- Step 5** Copy the new Version 6.2.1x software image to the WAE with the **copy ftp** command. You can use either Universal or Accelerator-only images.

```
wae# copy ftp install ftpserver / waas-image.bin
```



Note This example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.



Caution

If you are upgrading a vWAAS, ISR-WAAS, or SRE device from an earlier WAAS version to WAAS Version 6.2.1x, the upgrade process on this type of configuration will automatically clear system and data partition.

If you upgrade the vCM device to WAAS Version 6.2.1x via the console, a warning message similar to the following will be displayed:

```
WARNING: Upgrade of vCM device to 6.2.0 (or) higher version with '/sw' and '/swstore'
size less than 2GB will clear system and data partition.
```

If you upgrade the vCM device to WAAS Version 6.2.1x via the GUI, a warning message is not displayed.

- Step 6** Reload the WAE using the **reload** command.
- Step 7** Verify that the new Version 6.2.1x software image has installed correctly, using the **show version** command.
- Step 8** Verify that the correct licenses are installed, using the **show license** command.
- Step 9** If you have purchased an Enterprise license and have enabled it, proceed to Step 11.
If you have purchased an Enterprise license and have not yet enabled it, perform the following tasks:
- Clear the Transport license, using the **clear license transport** command.
 - Add the Transport license, using the **license add enterprise** command.
- Step 10** Save the changed configuration, using the **copy running-config startup-config** command.
- Step 11** From the primary WAAS CM, choose **Devices > branchWAE**, to verify that the WAE device is online and has a *green* status.
- Step 12** Verify the following WAE device functionalities:
- If you are using WCCP for traffic interception, verify that WCCP is working properly, using the **show running -config wccp** command.
 - (Optional) Confirm that flows are being optimized, using the **show statistics connection** command.
 - Confirm that the Enterprise license is enabled, using the **show license** command.
- If you have purchased the Enterprise license and it is enabled, proceed to [Step 13](#).
- If you have purchased an Enterprise license and have not yet enabled it, perform the following tasks:
- Clear the Transport license, using the **clear license transport** command.
 - Add the Enterprise license, using the **license add enterprise** command.

3. Save the changed configuration, using the **copy running-config startup-config** command.

Step 13 The branch WAE devices within the active WAAS network are now upgraded to the current WAAS Version 6.2.1x.

Upgrade Part 5: Upgrade the Data Center WAAS Software

Follow these steps to upgrade the data center WAAS software.

Step 1 Access the primary WAAS CM GUI:

`https://cm-ip-address`

Step 2 Verify that all WAE devices are online (displaying green).

Step 3 Resolve any alarm conditions that may exist.

Step 4 Upgrade each data center WAE ([Upgrade Part 6: Upgrade Each Data Center WAE](#)).



Note For deployments using WCCP as the traffic interception method, each data center WAE is automatically removed from the interception path. If your deployment does not use WCCP, use one of the following methods to remove each data center WAE from the interception path during the upgrade process:

For an inline deployment, use the interface `InlineGroup slot/grpnumber shutdown global configuration command` to bypass traffic on the active inline groups.

For a deployment using serial inline cluster, shut down the interfaces on the intermediate WAE in the cluster, then shut down the interfaces on the optimizing WAE in the cluster.

Upgrade Part 6: Upgrade Each Data Center WAE

Follow these steps to upgrade each data center WAE.

Step 1 Use the following sequence of commands to disable WCCP on the WAE and allow a graceful termination of existing TCP flows that are optimized by WAAS:

- a. Disable WCCP with the **no wccp tcp-promiscuous service-pair serviceID serviceID** global configuration command.
- b. Wait until the countdown expires, or use CTL-C to skip the countdown.
- c. Verify that WCCP is disabled, using the **show wccp status** command.
- d. Save the changed configuration, using the **copy running-config startup-config** command.

Step 2 (Optional) Disable WCCP on the intercepting router or switch, using the **no ip wccp** global configuration command.



Note We recommend this step only if the Cisco IOS release on the router or switch has not been scrubbed for WCCP issues for your specific platform.

Step 3 (Optional) Verify that WCCP is disabled, using the **show ip wccp** command, if you have used [Step 2](#).

Step 4 Upgrade the data center WAE software:

- a. Open a console session or Telnet to the branch WAE.
- b. Copy the new Version 6.2.1x software image to the WAE with the **copy ftp** command. You can use either Universal or Accelerator-only images.

```
waec# copy ftp install ftpserver / waas-image.bin
```



Note This example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.

- c. Reload the WAE using the **reload** command.
- d. Verify that the new Version 6.2.1x software image has installed correctly, using the **show version** command.
- e. Verify that WCCP is disabled, using the **show wccp status** command.
- f. Save the changed configuration, using the **copy running-config startup-config** command.

Step 5 From the primary WAAS CM, choose **Devices > branchWAE**, to verify that the WAE device is online and has a *green* status.

Step 6 (Optional) Enable WCCP on all intercepting routers or switches in the list, if you have used [Step 2](#).

- a. Telnet to each core router or switch.
- b. Enable WCCP, using the **ip wccp 61 redirect-list acl-name** command and the **ip wccp 62 redirect-list acl-name** command.
 - WCCP Service ID 61—Source IP address. The WCCP Service ID (service group) is applied closest to the LAN interface.
 - WCCP Service ID 62—Destination IP address. The WCCP Service ID (service group) is applied closest to the WAN interface.
 - You can change the WCCP redirect list as needed by changing the redirect in/out statement.

Step 7 Verify the following WAE device functionalities:

- a. Enable WCCP, using the **wccp tcp-promiscuous service-pair serviceID serviceID** global configuration command. If you are using WCCP single-service, use the **wccp tcp-promiscuous serviceID** global configuration command.
- b. Verify that redirecting router IDs are seen, using the **show wccp routers** command.
- c. Verify that all WAAs in the cluster are seen, using the **show wccp clients** command.
- d. Verify that the packet count to the WAE is increasing and no loops are detected, using the **show wccp statistics** command.
- e. Verify that the buckets assigned for Service Group 61 match those of Service Group 62, and are assigned to the WAE, using the **show wccp flows tcp-promiscuous detail** command.
- f. Verify that flows are being optimized, using the **show statistics connection** command.

- g. If you are using WCCP for traffic interception, verify that WCCP is working properly, using the **show running -config wccp** command.

Step 8 Each data center WAE within the active WAAS network is now upgraded to the current WAAS Version 6.2.1x.

Upgrade Part 7: WCCP and Migration Processes

For information on the sets of tasks to enable and reconfigure WCCP, and information on configuring accelerators, switches and routers for migration, see the [Cisco Wide Area Application Services Upgrade Guide](#).

Upgrade Part 8: Post-Upgrade Tasks

Perform the following tasks after you have completed the upgrade to WAAS Version 6.2.1x:

- After upgrading a Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.
- 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 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 use the setup utility for basic configuration after upgrading to 6.2.1x, WCCP router list 7 is used. Because the setup utility is designed for use on new installations, any existing configuration for WCCP router list 7 is replaced with the new configuration.
- If you have 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 6.2.1x, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords. If you do not reenter the passwords, after upgrading to Version 6.2.1x, 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 6.2.1x, 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.

Migrating a WAAS CM from an Unsupported to a Supported Platform

If you have a Cisco WAAS Central Manager that is running on a hardware platform that is unsupported in Version 6.1 and later (such as a WAE-274/474/574/674/7341/7371), you are not allowed to upgrade the device to Version 6.1 or later. You must migrate the WAAS CM to a supported platform by following the procedure in this section, which preserves all of the WAAS CM configuration and database information.



Caution

Database backup is intended for recovery of the current WAAS CM only. Restoring to a different device will retain the device identity and will not allow you to re-use the current hardware in a different role. If you want to migrate the service to a new device, register the device as a standby WAAS CM first, and then change its role after database synchronization.

Follow these steps to migrate a primary WAAS CM from an unsupported platform to a platform that is supported for WAAS Version 6.2.1x:

- 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-03-18-2016-15-08_5.0.1.0.15.dump
Backup file backup/cms-db-03-18-2016-15-08_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-03-18-2016-15-08_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 6.1. 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-03-18-2016-15-08_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-03-18-2016-15-08_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, 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-03-18-2016-15-08_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 6.2.1x. You can use the Central Manager Software Update window or the **copy ftp install** command.

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

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

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

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

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

## Migrating a Physical Appliance Being Used as a WAAS CM to a vCM

Follow these steps to migrate a physical appliance being used as a primary WAAS CM to a vCM:

- 
- Step 1** Introduce vCM as the Standby Central Manager by registering it to the Primary Central Manager.
  - Step 2** Configure both device and device-group settings through Primary CM and ensure that devices are getting updates. Wait for two to three data feed poll rate so that the Standby CM gets configuration sync from the Primary CM.
  - Step 3** Ensure that the Primary CM and Standby CM updates are working.
  - Step 4** Switch over CM roles so that vCM works as Primary CM. For more information, see the “Converting a Standby Central Manager to a Primary Central Manager” section of the [Cisco Wide Area Application Services Configuration Guide](#).
- 

## Ensuring a Successful RAID Pair Rebuild

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



### Caution

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

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

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

- The device is offline in the Central Manager GUI.
- CMS cannot be loaded.
- Error messages say that the file system is read-only.
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” or “ext3\_readdir: bad entry in directory.”
- Other unusual behaviors occur that are related to disk operations or the inability to perform them.

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

## Downgrading from Version 6.2.1x to a Previous Version

This section contains the following topics:

- [Downgrading the WAAS System from Version 6.2.1x to a Previous Version](#)
- [Downgrading the WAAS CM from Version 6.2.1x to a Previous Version](#)

## Downgrading the WAAS System from Version 6.2.1x to a Previous Version

This section contains the following topics:

- [Downgrade Path Considerations](#)
- [Downgrade Component and Data Considerations](#)

### Downgrade Path Considerations

- Downgrading from 6.2.1x is supported to 6.1.1a, 6.1.1, 5.5.5a, 5.5.5 and 5.5.3. Downgrading directly from 6.x to a version earlier than 5.5.3 is not supported.
- 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.
- On WAVE-294/594//8541 models with solid state drives (SSDs) you cannot downgrade to a version earlier than 5.2.1.
- On WAVE-694 model with solid state drives (SSDs), you cannot downgrade to a version earlier than 5.5.1.
- On vCM-500/vCM-1000, you cannot downgrade to a version earlier than 5.5.1.

### Downgrade Component and Data Considerations

- 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.
- Current BMC (Baseboard Management Controller) settings are erased and restored to factory default settings when you downgrade Cisco WAAS to a version earlier than 4.4.5.
- If you have configured disk cache for ISR-WAAS device, downgraded from 6.1.1x to 5.5.3, and then restore rollback to 6.1.1x, you must reload the disk cache configuration for the new configuration to take effect. If you do not perform a reload after the rollback to 6.1.1x, the new configuration will not take effect, and output from the show disks cache-details command will display the error message "Disk cache has been configured. Please reload for the new configuration to take effect."

## Downgrading the WAAS CM from Version 6.2.1x to a Previous Version

This section contains the following topics:

- [WAAS CM Downgrade Path Considerations](#)
- [WAAS CM Downgrade Procedure Considerations](#)
- [Procedure for Downgrading the WAAS CM to a Previous Version](#)

## WAAS CM Downgrade Path Considerations

- Downgrading the WAAS CM to a version earlier than Version 5.5.3 is blocked.
- 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.
- When downgrading a WAAS CM to a version earlier than 4.4.1, and secure store is in auto-passphrase mode, the downgrade is blocked. You must switch to user-passphrase mode before you can downgrade to a software version that does not support auto-passphrase mode.

## WAAS CM Downgrade Procedure Considerations

- As it applies to your WAAS CM and the current version of your WAAS system, perform the following tasks *before* a WAAS CM downgrade:
  - If you have a standby Central Manager, it must be registered to the primary Central Manager *before* the downgrade.
  - Prior to downgrading the WAAS CM to a version up to 5.2.1, you must remove Backup WNG from the AppNav-XE cluster and verify that the WAAS CM and AppNav-XE device are in sync.
  - Before downgrading to a version earlier than 4.4.1, we recommend that you change the following WCCP parameters, if they have been changed from their default values:
    - Change service IDs back to their default values of 61 and 62.
    - Change the failure detection timeout back to the default value of 30 seconds.




---

**Note** Only these WCCP default values are supported in versions prior to 4.4.1; 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.

---

- Each of the following WAAS CM downgrade procedures requires a particular task sequence:
  - If the WAAS CM is downgraded to a version up to 5.2.1 and if the AppNav-XE cluster has more than 32 WAAS nodes: prior to downgrade, we recommend that you reduce the number of WAAS nodes to a maximum of 32 WAAS nodes.
  - 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.
- When downgrading an AppNav Controller device to a version earlier than 5.0.1, you must perform the following tasks:
  1. Deregister the device from the WAAS CM.
  2. Change the device mode to application-accelerator.
  3. Downgrade the device.

4. Re-register the device (or, alternatively, 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.




---

**Note** 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.

---

## Procedure for Downgrading the WAAS CM to a Previous Version

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-03-18-2016-15-08_5.0.1.0.15.dump
Backup file backup/cms-db-02-18-2016-15-08_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-03-18-2016-15-08_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
```




---

**Note** After downgrading a WAAS CM, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.

---

- Step 3** Reload the device.




---

**Note** Downgrading the database may trigger full updates for registered devices. In the WAAS CM 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 6.2.1xx:

- **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 and do not reach the limit of the HTTP object cache.

- **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.

- **HTTP Object Cache and Akamai Connect**

HTTP application optimization with Akamai Connect (HTTP object cache) may deliver unexpected HTTP objects to a client, which may create a risk of delivering malicious content. This scenario can occur after a different—erroneously configured, or otherwise failing—client device has retrieved the object with a matching URL from an invalid HTTP server. A check for this scenario will be implemented in a future WAAS release.

## Device Group Default Settings

When you create a device group in WAAS Version 6.2.1x, the Configure > Acceleration > DSCP Marking page is automatically configured for the group, with the default DSCP marking value of copy.

- **Using Autoregistration with Port-Channel 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.

## CIFS Support of FAT32 File Servers

The CIFS accelerator does not support file servers that use the FAT32 file system. You can use the policy rules to exclude from acceleration any file servers that use the FAT32 file system.

## Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP

When using the Cisco ASR 1000 Series router and WCCP to redirect traffic to a WAE that is using WCCP GRE return as the egress method and the HTTP accelerator is enabled, there may be an issue with HTTP slowness due to the way the ASR router handles proxied HTTP connections (see [CSCtj41045](#)). To work around this issue, on the ASR router, create a web cache service in the same VRF as that of the 61/62 service by using the following command: **ip wccp [vrf vrf-name] web-cache**

- **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.

## Configuring SMART-SSL Acceleration

SMART-SSL is an encryption service that enables L7 application network services ( e.g. ftp, http, dns) to optimize traffic on SSL/TLS encrypted connections. It enables content caching for SSL/TLS applications (http object cache for https traffic) in single sided deployment.

With the evolution of cloud services, there is a critical need to provide application optimization in a single-sided deployment scenario. With SMART-SSL optimization, the interposing device does not require a peer device to process the SSL traffic flow. SSL traffic can be optimized by the edge device without having to go through a core device.

This section contains the following topics:

- [Preparing to Use SMART-SSL Acceleration](#)
- [Creating a Root CA certificate](#)
- [Creating Single-Sided SSL Accelerated Service Certificate](#)
- [Configuring and Enabling SMART-SSL Accelerated Services on Single-Sided Device Group](#)

Table 7 provides an overview of the steps you must complete to set up and enable SMART-SSL acceleration.

*Table 7 Checklist for Configuring SMART-SSL Acceleration*

| Task                                              | Additional Information and Instructions                                                                                                                                                                                                                    |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Prepare for configuring SSL acceleration.      | Identifies the information that you need to gather before configuring SSL acceleration on your WAAS devices. For more information, see <a href="#">Preparing to Use SMART-SSL Acceleration</a> .                                                           |
| 2. Set up Root CA certificates                    | (Optional) Describes how to create, import, and manage certificate authority (CA) certificates. For more information, see <a href="#">Creating a Root CA certificate</a> .                                                                                 |
| 3. Set up accelerated service certificates.       | Describes how to create, import, and use certificates for SMART-SSL acceleration. For more information, see <a href="#">Creating Single-Sided SSL Accelerated Service Certificate</a> .                                                                    |
| 4. Configure and enable SSL-accelerated services. | Describes how to add, configure, and enable services to be accelerated by the SMART-SSL application optimization feature. For more information, see <a href="#">Configuring and Enabling SMART-SSL Accelerated Services on Single-Sided Device Group</a> . |

## Preparing to Use SMART-SSL Acceleration

Before you configure SMART-SSL acceleration, you should know the following information:

- The services that you want to be accelerated on the SMART-SSL traffic. You will need to create a certificate to optimize these services using their urls.
- The server IP address and port information.
- The public key infrastructure (PKI) certificate and private key information, including the certificate common name and CA-signing information.
- The SSL versions supported.  
SSLv3, TLS1.0-1.2 are supported with this release.

- Supported ciphers

The following lists the twenty seven supported ciphers:

```

TLS_RSA_WITH_3DES_EDE_CBC_SHA, /* 0x000A */
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA, /* 0x0016 */
TLS_RSA_WITH_AES_128_CBC_SHA, /* 0x002F */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, /* 0x0033 */
TLS_RSA_WITH_AES_256_CBC_SHA, /* 0x002F */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, /* 0x0039 */
TLS_RSA_WITH_AES_128_CBC_SHA256, /* 0x003C */
TLS_RSA_WITH_AES_256_CBC_SHA256, /* 0x003D */
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA, /* 0x0041 */
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA, /* 0x0045 */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, /* 0x0067 */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, /* 0x006B */
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0084 */
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0088 */
TLS_RSA_WITH_SEED_CBC_SHA, /* 0x0096 */
TLS_DHE_RSA_WITH_SEED_CBC_SHA, /* 0x009A */
TLS_RSA_WITH_AES_128_GCM_SHA256, /* 0x009C */
TLS_RSA_WITH_AES_256_GCM_SHA384, /* 0x009D */
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, /* 0x009E */
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, /* 0x009F */
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, /* 0xC012 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, /* 0xC013 */

```

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, /* 0xC014 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, /* 0xC027 */
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, /* 0xC028 */
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, /* 0xC02F */
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 /* 0xC030 */
```

## Creating a Root CA certificate

A root SSL certificate is a certificate issued by a trusted certificate authority and is in turn trusted by domain clients. This is used to sign all issued certificates. This CA needs to be capable of accepting certificate signing requests (CSRs) that include subject alternative names and generate certificates that include subject alternative names. The subject alternative name is an extension to the X.509 protocol that allows various values to be associated with a security certificate (SSL certificate). Subject alternative names can include IP addresses, email addresses, universal resource identifiers (URIs), alternative common Domain Name System (DNS) names, alternatives to the distinguished name, and other information. You can install this on all machines that will be communicating with services using SSL certificates generated by this root certificate. If your organization already has a root CA for its internal use, you can use it instead of a new root CA. If not, use a Linux machine with openssl version of 1.0.1e or greater to create these certificates.

- 
- Step 1** Create the root CA key. This signs all issued certificates.  

```
openssl genrsa -out rootCA.key.pem 2048
```
  - Step 2** Create the self-signed root CA certificate, with the key generated above.  

```
openssl req -x509 -new -nodes -key rootCA.key -days 365 -out rootCA.crt.pem
```
  - Step 3** Verify the root certificate.
  - Step 4** Import the certificate from the Enterprise CA to the Trusted Root Certification Authorities store on the client browser and install the root CA certificate and intermediate CA certificate.

## Creating Single-Sided SSL Accelerated Service Certificate

To create the certificate to be used with the accelerated service, follow the steps below:

- 
- Step 1** Create a new encryption key pair using open ssl.  

```
openssl genrsa -out proxyserver.key 1024
```
  - Step 2** Create a Certificate Signing Request (CSR) and key pair and other needed attributes such as Common Name, Company and SubjAltName for the application you are trying to optimize. For example, in case of YouTube(TM), make sure the subjectAltNames have all the URLs that YouTube(TM) servers include in their certificate that you would like to optimize.  

```
openssl req -new -key server.key -out server.csr
```

```
X509v3 extensions:
 X509v3 Basic Constraints:
 CA:FALSE
 Netscape Comment:
 NGSSL Demo Certificate
 X509v3 Subject Key Identifier:
 65:C1:42:98:47:81:0E:04:7A:7D:83:A7:43:C9:A3:B8:1F:DB:BF:1E
 X509v3 Authority Key Identifier:
 keyid:8C:F6:0A:BC:E4:EB:2C:D9:6B:68:95:09:1B:B5:82:66:CE:ED:6B:77
 X509v3 Subject Alternative Name:
```

```
DNS:*google-analytics.com, DNS:*google.com, DNS:*google.com,
DNS:*googleadservices.com, DNS:*googleapis.com, DNS:*googlesyndication.com,
DNS:*googletagmanager.com, DNS:*googlevideo.com, DNS:*gstatic.com,
DNS:*youtube-nocookie.com, DNS:*youtube.com, DNS:*yimg.com, DNS:ad.doubleclick.net,
DNS:doubleclick.net, DNS:google-analytics.com, DNS:google.com, DNS:googleadservices.com,
DNS:googleapis.com, DNS:googlesyndication.com, DNS:googletagmanager.com,
DNS:googletagservices.com, DNS:googlevideo.com, DNS:gstatic.com, DNS:youtube-nocookie.com,
DNS:youtube.com
```

**Step 3** Create new proxy server certificate by signing the above generated CSR with your enterprise root CA, created above. This will generate .crt or .pem certificate file.

Note that the CA certificate used to sign this accelerated service certificate should be present in the client browser root CA store for the accelerated service proxy certificate created to be authenticated and accepted by the client browser.

- IE or Chrome: settings- advanced settings - certificates - import - add the root ca -into trusted root authorities. Clear the browser cache and reload the browser for the cloud application and it should pick up the new certificate.
- Mozilla: options - advanced - Certificates> View certificates > Import - click all the three for the trusted zones and import the certificate. Clear the browser cache and reload the browser for the cloud application and it should pick up the new certificate.

**Step 4** WAAS allows importing certificates s only with pkcs12 format. To generate the pcks12 format from the certificate file and your private key use the open ssl command.

```
openssl pkcs12 -export -out server.p12 -inkey proxyserver.key -in proxyserver.crt
-certfile CACert.crt
```

**Step 5** Import this certificate into the WAAS device group using **crypto import EXEC** command and thereafter be used in the accelerated server configuration as server-cert-key.

```
WAE#crypto import pkcs12 newcert.p12 pkcs12
```

It is important to note that the CA cert used to sign this ASVC cert will need to exist in the browser rootCA store for the accelerated service proxy certificate create to be authenticated and accepted by the browser.

## Configuring and Enabling SMART-SSL Accelerated Services on Single-Sided Device Group

The following are prerequisites for using Cisco WAAS to optimize SSL Interposer/Optimizer v2 traffic:

- The Central Manager and WAEs must be running software version 6.2.x. For information, see the “Obtaining the Latest Software Version from Cisco.com” section of the “Maintaining Your WAAS System” chapter of the *Cisco Wide Area Application Services Configuration Guide*.
- A new device group that will support single-sided acceleration. For information on creating device groups, see the “Creating a Device Group” section of the “Using Device Groups and Locations” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

After you have created an accelerated service certificate for WAN optimization, to enable the SSL Interposer/Optimizer v2 settings on this group follow these steps:

**Step 1** From the WAAS Central Manager menu, choose **Device Groups** > *device-group-name*, to select the device group created above. Add only branch devices to this group. These devices will optimize the SSL traffic as it passes through them.

**Step 2** Choose **Configure** > **Acceleration** > **Enabled Features**.

- Step 3** Check the **SSL Interposer** check box to enable SSL Optimizer v2 acceleration. Alternately, use the accelerator interposer-ssl enable global configuration command from the CLI to enable SSL Optimizer v2 acceleration.
- Step 4** Create an SSL accelerated service for the device group. Choose **Acceleration > SSL Accelerated Services** and click the **Create** button. The **Creating New SSL Accelerated Service** page opens.
- Step 5** In the SSL Accelerated Service section, name your service, and select both **In Service** and **Match Server Name Indication** boxes. You can also provide a short description.
- Step 6** In the Server Addresses section, enter “any” in the **IP Address** box and “443” in the **Server Port** box. Then click **Add**.
- Step 7** In the **Certificate and Private Key** section, click **Import Existing Certificate and Optionally Private Key** and select **Upload File in PKCS#12 Format**. Supply the password used to export the certificate ( Using the **Browse** button, locate the certificate. Then click the **Import** button. A confirmation screen with the certificate information appears.
- Step 8** Click **Submit** to complete configuring the SSL-accelerated service to use single sided optimization. Alternatively, if you want to automate the entire process using a script, we recommend that you get in touch with the Cisco Technical Assistance Center (TAC).
- Step 9** Monitor the accelerated service optimization statistics using the Cisco WAAS Central Manager and the command-line interface (CLI) using the **show statistics connections optimized** exec command.

## Software Version 6.2.1x Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, and command changes in Software Version 6.2.1x, fixed and known and contains the following topics:

- [Cisco Software Version 6.2.1a Resolved Caveats](#)
- [Cisco Software Version 6.2.1 Resolved Caveats](#)
- [Cisco Software Version 6.2.1 Open Caveats](#)
- [Cisco Software Version 6.2.1x Command Changes](#)
- [Using Previous Client Code](#)

### Cisco Software Version 6.2.1a Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.1a.

| Caveat ID Number           | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCuy55846</a> | WAAS 6.1.1a SMB AO restart generating core file                          |
| <a href="#">CSCuy59549</a> | WAAS 6.1.1a SMB AO core file on DC device                                |
| <a href="#">CSCuy06186</a> | LAN devices are not accessible after shutting port-channel mem interface |

| Caveat ID Number           | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCva02503</a> | Serial-to-IP converter packets dropped by WAAS 6.1 with inline           |
| <a href="#">CSCva30228</a> | WAAS cons are retransmitting packets very quickly and are getting reset. |

## Cisco Software Version 6.2.1 Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.1.

| Caveat ID Number           | Headline                                                                                 |
|----------------------------|------------------------------------------------------------------------------------------|
| <a href="#">CSCus23919</a> | Cisco WAAS Appliances may be vulnerable to published vulnerabilities                     |
| <a href="#">CSCuv88935</a> | Java process may reload when waasnet is in unexpected state.                             |
| <a href="#">CSCuw54689</a> | The number of pending connections is not updated in sh stat tfo                          |
| <a href="#">CSCuw92521</a> | imeout of all the AO's are seen during the SOAK testing                                  |
| <a href="#">CSCux21918</a> | WAAS device will periodically save the running configuration with PCM off                |
| <a href="#">CSCux23101</a> | 64bit binaries in /swstore/unstripped are stripped                                       |
| <a href="#">CSCux24107</a> | Logs of acc_proxy services are not rotated                                               |
| <a href="#">CSCux29290</a> | Inbuilt Packet Capture on WAAS does not filter by ACL                                    |
| <a href="#">CSCux29322</a> | Inbuilt Packet Capture does not work on WAAS CM                                          |
| <a href="#">CSCux36901</a> | ICA AO can generate a core file and restart                                              |
| <a href="#">CSCux40718</a> | Inaccurate data in waas express statistics                                               |
| <a href="#">CSCux45852</a> | Error when registering router with duplicate certificate is "failed"                     |
| <a href="#">CSCux46706</a> | WCM 5.5.3 showing peak and active connections greater than device limit                  |
| <a href="#">CSCux50167</a> | Inaccurate WAN offload stat in Top Sites report                                          |
| <a href="#">CSCux72976</a> | OC_Server core observed in ISR-WAAS when reloading the Router                            |
| <a href="#">CSCux96577</a> | Packet capture filters not working in a specific case                                    |
| <a href="#">CSCux99224</a> | Connection reset observed when sending SMBv2 traffic from samba client to win2k12 server |
| <a href="#">CSCuy06208</a> | IPv4 Gateway is not reachable in Dual stack scenario.                                    |
| <a href="#">CSCuy25131</a> | Unable to run AppNav-XE registration from WAAS CM                                        |
| <a href="#">CSCuy42636</a> | TFO performance is slow with packet drop                                                 |
| <a href="#">CSCuy46550</a> | Disk failed alarm is not triggered for Offline disk in 8541 device                       |
| <a href="#">CSCuy58094</a> | Evaluation of waas for OpenSSL March 2016                                                |
| <a href="#">CSCuy61286</a> | SMB PP: preposition of files getting errored out with IO_TIMEOUT                         |
| <a href="#">CSCuy75712</a> | CLI failed msgs seen after registering ISR-WAAS to CM                                    |
| <a href="#">CSCuy80989</a> | Custom syslog dest port results in random dest port                                      |

| Caveat ID Number           | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCuy82550</a> | Memory leak seen with continuous SNMP MIB polling                        |
| <a href="#">CSCuz08541</a> | WAAS failing to display connections and intermittent connection failures |

## Cisco Software Version 6.2.1 Open Caveats

The following caveats are open in Software Version 6.2.1.

| Caveat ID Number           | Headline                                                                  |
|----------------------------|---------------------------------------------------------------------------|
| <a href="#">CSCvc17689</a> | Incorrect destination MAC address for optimized traffic to AppNav router  |
| <a href="#">CSCuz55707</a> | All devices cannot use CM as proxy for http object cache                  |
| <a href="#">CSCuy06186</a> | LAN devices are not accessible after shutting port-channel mem interface. |
| <a href="#">CSCuy06942</a> | ISR-WAAS: SMB accelerator gets disabled upon ISR router upgrade/reload    |
| <a href="#">CSCuy55214</a> | Gateway is unreachable when port-channel has more than 2 interfaces       |
| <a href="#">CSCuy58094</a> | Evaluation of waas for OpenSSL March 2016                                 |
| <a href="#">CSCuz10327</a> | File transfer failed in a specific scenario in Azure vWAAS                |
| <a href="#">CSCuz22537</a> | SMB Preposition tasks with multiple domains fail when run in parallel     |
| <a href="#">CSCuz34038</a> | ISR-WAAS goes offline after long duration traffic                         |
| <a href="#">CSCuz37952</a> | MAPI : Connections getting dropped while sending large attachment mails   |
| <a href="#">CSCuz41637</a> | Rarely policy engine doesn't push connection to HTTP AO during upgrade    |
| <a href="#">CSCuz47571</a> | Akamai:Object-Cache top-hosts counters are not getting incremented        |
| <a href="#">CSCuz49231</a> | sshd login to Azure vWAAS not working                                     |
| <a href="#">CSCuz55377</a> | File invalidation issue with write operation in 2.1 dialect in Azure      |
| <a href="#">CSCus23919</a> | Cisco WAAS Appliances may be vulnerable to published vulnerabilities      |
| <a href="#">CSCut83135</a> | Core.dispatcher file created while configuring machine account identity   |
| <a href="#">CSCux76467</a> | Outlook not connect to exchange with Wan secure interoperable mode        |
| <a href="#">CSCux94938</a> | ce_cache_unusable alarm seen with Akamai enabled                          |
| <a href="#">CSCuy03541</a> | ce_cache_unusable alarm in vWAAS during Upgrade and Migration             |
| <a href="#">CSCuy46644</a> | Interception access-list not working, connections getting pass-through    |
| <a href="#">CSCuy73435</a> | SMB preposition task may get fail when running more than 15 in parallel   |
| <a href="#">CSCuz11211</a> | AO Timeouts seen during longevity test                                    |
| <a href="#">CSCuz12323</a> | Force device group not pushing enable feature config in specific scenario |
| <a href="#">CSCuz18923</a> | preinstall script does not check current version for supported upgrade    |
| <a href="#">CSCuz39661</a> | service-insertion swap src-ip feature doesnt required config match SC&SN  |
| <a href="#">CSCuz42604</a> | Akamai:"Could not write statistics value to ts_thrift_stats_uds" error    |
| <a href="#">CSCuz55920</a> | Empty server response found in Web-Pages in a specific scenario           |
| <a href="#">CSCuz59552</a> | Akamai: Preposition logging missing, PP-IMS sometimes doesn't happen.     |



| Caveat ID Number           | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCuy30007</a> | SMB Preposition does not support Extended Unicode Characters             |
| <a href="#">CSCuz61982</a> | SMBAO preposition is not working with NetApp filer with SMBv2 Signing    |
| <a href="#">CSCuw17054</a> | MAPI AO gets disabled and MAPI Core observed for RPC-HTTPS with Kerberos |
| <a href="#">CSCuz15000</a> | vWAAS-Azure pending Development from Microsoft                           |
| <a href="#">CSCux30779</a> | SMB Preposition task status shows completed if connection not optimized  |

## Cisco Software Version 6.2.1x Command Changes

This section lists the new and modified commands in Cisco WAAS Software Version 6.2.1x.

[Table 8](#) lists the commands and options that have been added or changed in Cisco WAAS Software Version 6.2.1x.

**Table 8** CLI Commands Added or Modified in Version 6.2.1x

| Mode                      | Command                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global configuration      | <b>(config) accelerator http preposition proxy server</b> | Configures a proxy server that can be used by an HTTP/S preposition task.                                                                                                                                                                                                                                                                                                                                                                             |
|                           | <b>(config) device mode</b>                               | New <b>application-accelerator profile branch</b> parameter added, with WAVE-7541, WAVE-7571 and WAVE-8541, which enables the device to function as a branch device, to configure resource pre-allocation resources for various WAAS services to be branch traffic scenario and branch services.<br><br>The branch profile-enabled connection count used for computing memory for pre-allocation is 3/4 of the TFO limit for WAVE-7571 and WAVE-8541. |
|                           | <b>(config) interception-method</b>                       | The <b>interception-method inline</b> global configuration command is now also available on the vWAAS platform.                                                                                                                                                                                                                                                                                                                                       |
|                           | <b>(config) accelerator smb preposition</b>               | Creates a smb preposition directive.                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                           | <b>(config) accelerator smb dre</b>                       | Enables DRE for smb preposition tasks.                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preposition configuration | <b>(config-preposition) use-proxy</b>                     | Enables proxy use by a specific preposition task.                                                                                                                                                                                                                                                                                                                                                                                                     |
|                           | <b>(config-preposition) user-agent</b>                    | Creates a user agent to display information about the client browser and operating system used to access the URLs specified for a preposition task.                                                                                                                                                                                                                                                                                                   |
| EXEC                      | <b>crypto generate</b>                                    | Added new Usage Guidelines for RSAS modulus for a self-signed certificate.                                                                                                                                                                                                                                                                                                                                                                            |
|                           | <b>debug accelerator</b>                                  | Updated with new keyword RPCHTTP-layer                                                                                                                                                                                                                                                                                                                                                                                                                |
|                           | <b>show accelerator mapi</b>                              | Updated example to show the status of the RPC HTTP optimization field.                                                                                                                                                                                                                                                                                                                                                                                |
|                           | <b>show accelerator smb</b>                               | Updated example to show Highest Dialect 3_02                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 8 CLI Commands Added or Modified in Version 6.2.1x (continued)

| Mode | Command                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <b>show device-mode</b>                        | New <b>profile-branch</b> parameter added.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|      | <b>show statistics accelerator smb</b>         | The following new fields are added to this command's output <ul style="list-style-type: none"> <li>• Total Number of SMB3_0 Encrypted Sessions (L4 opt)</li> <li>• Total Number of SMB3_0 Encrypted Sessions (L7 opt)</li> <li>• Total Number of SMB3_02 Encrypted Sessions (L4 opt)</li> <li>• Total Number of SMB3_02 Encrypted Sessions (L7 opt)</li> <li>• Total Number of Encrypted Requests Processed</li> <li>• Total Number Encrypted of Requests Served Locally</li> <li>• Total Number of Encrypted Requests Sent to File Servers</li> <li>• Total Number of Encrypted SMB Bytes read from LAN (Original)</li> <li>• Total Number of Encrypted SMB Bytes written to LAN (Original)</li> </ul> |
|      | <b>show statistics accelerator mapi detail</b> | The following new fields are added to this command's output. <ul style="list-style-type: none"> <li>• Number of active IN channels</li> <li>• Number of active OUT channels</li> <li>• Number of active optimized sessions</li> <li>• Number of active RPC HTTP(S) clients</li> <li>• Number of RPC HTTP connections optimized since uptime</li> <li>• Number of Handled RPCH Virtual Sessions</li> <li>• Number of Optimized RPCH Virtual Sessions</li> <li>• Number of Pipe-through Virtual Sessions</li> </ul>                                                                                                                                                                                       |

## Using Previous Client Code

If you have upgraded to Cisco WAAS Version 6.2.1x 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/CADDBeanTemplateHeader.xsl
org/apache/axis2/schema/template/CADDBeanTemplateSource.xsl
org/apache/axis2/schema/template/PlainBeanTemplate.xsl
org/apache/axis2/schema/template/ADDBeanTemplate.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 ADDBeanTemplate.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.



**Note** IOS-XE 3.14 should not be used for ISR-WAAS.

## 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](#)
- [Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series](#)
- [Installing the Cisco WAE Inline Network Adapter](#)

# Obtaining Documentation and Submitting a Service Request

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

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

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

---

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

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.

© 2019 Cisco Systems, Inc. All rights reserved.

